

“ . . . to insure domestic Tranquility,  
provide for the common defence . . . ”

PAPERS FROM THE CONFERENCE ON  
HOMELAND PROTECTION

Edited by  
Max G. Manwaring

October 2000

\*\*\*\*\*

The views expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. This report is cleared for public release; distribution is unlimited.

\*\*\*\*\*

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave., Carlisle, PA 17013-5244. Copies of this report may be obtained from the Publications and Production Office by calling commercial (717) 245-4133, FAX (717) 245-3820, or via the Internet at rummelr@awc.carlisle.army.mil

\*\*\*\*\*

Most 1993, 1994, and all later Strategic Studies Institute (SSI) monographs are available on the SSI Homepage for electronic dissemination. SSI's Homepage address is: <http://carlisle-www.army.mil/usassi/welcome.htm>

\*\*\*\*\*

The Strategic Studies Institute publishes a monthly e-mail newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please let us know by e-mail at [outreach@awc.carlisle.army.mil](mailto:outreach@awc.carlisle.army.mil) or by calling (717) 245-3133.

ISBN 1-58487-036-2

## CONTENTS

Foreword . . . . .	v
Overview <i>Max G. Manwaring</i> . . . . .	1
1. A Strategic Perspective on U. S. Homeland Defense: Problem and Response <i>John J. Hamre</i> . . . . .	11
2. The Army of the Constitution: The Historical Context <i>Gregory J.W. Urwin</i> . . . . .	27
3. The Public's Expectations of National Security <i>Peter D. Feaver</i> . . . . .	63
4. Security Expectations for Transnational Corporations <i>George K. Campbell.</i> . . . . .	75
5. Ballistic and Cruise Missile Threats <i>Steven A. Cambone</i> . . . . .	85
6. Chemical and Biological Terrorism: Political Hype or Bona Fide Post-Cold War Threat? <i>Russell Howard</i> . . . . .	99
7. Infrastructure Warriors: A Threat to the U.S. Homeland by Organized Crime <i>Thomas A. Johnson</i> . . . . .	161

8. Threat of Civil Unrest and Insurrection	
<i>William A. Navas, Jr.</i> . . . . .	171
9. Missile Defense	
<i>John Costello</i> . . . . .	181
10. Evolving Roles and Missions for the Reserve Components in Responding to Incidents Involving Weapons of Mass Destruction	
<i>Ellen Embrey</i> . . . . .	191
11. In Support of the Civil Authorities	
<i>Donald A. Haus.</i> . . . .	199
12. Where Domestic Security and Civil Liberties Collide	
<i>Charles J. Dunlap, Jr.</i> . . . .	209
13. A Strategic View of Where the Army Is: Homeland Defense and Issues of Civil- Military Relations	
<i>Don M. Snider</i>	
<i>John A. Nagl</i>	
<i>Tony Pfaff.</i> . . . .	229
14. Toward a National Security Policy and Strategy for Now and the 21st Century	
<i>Edwin G. Corr</i>	
<i>Max G. Manwaring</i> . . . . .	261
About the Contributors . . . . .	273

## FOREWORD

On April 11-13, 2000, the U.S. Army War College Strategic Studies Institute sponsored a major conference that examined what the Department of Defense must do “to insure domestic Tranquility, provide for the common defence . . .,” given the increasing contemporary threats to the U.S. homeland. The conference drew on the creative thinking of over 200 U.S. and foreign academic, business, civilian, governmental, and military leaders. The discussions generated an exceptionally rich exchange of information and ideas concerning problems and solutions to U.S. national security for now and into the 21st century. In general, the conference discussions revolved around four salient and interrelated issues: the historical context for dealing with threats to the American homeland; the complex threat situation; the evolving strategy and structure for homeland defense; and some critical considerations and recommendations.

This book highlights the issues and themes that ran through the conference. As such, it is not a comprehensive record of the proceedings. It is organized as an anthology of the best of a series of outstanding conference presentations, revised in light of the discussions that took place there. Finally, the anthology is complemented by an overview and four specific recommendations. Those recommendations look to the future and place emphasis on the transformation strategy that conference participants considered essential to safeguard the American homeland now and into the future.

We have not attempted to provide all the answers. Rather, our intention is to stimulate and facilitate a wider and more profound debate on U.S. defense priorities, and the need for a paradigm shift to meet the compound complex challenges of the contemporary national and global security environment. Such a debate will be critical in building the necessary support of the Congress, the Defense Commu-

nity, and the American people for the extensive changes that must be undertaken. We hope that the insights, concerns, and recommendations found in this anthology will help build a strong consensus for regenerating national security thinking, policy, strategy, and structure to meet the needs and threats of the next century. If we achieve that, we will have fulfilled our mission and commitment to you (the reader), the Department of Defense, and the American people.

DOUGLAS C. LOVELACE, JR.  
Director  
Strategic Studies Institute

# OVERVIEW

Max G. Manwaring

Protecting the territory and interests of the United States and its citizens from “all enemies both foreign and domestic . . .,” and “to insure domestic Tranquility . . .” are the principal tasks of government. The primary reason to emphasize homeland defense is the change in the type, degree, and number of threats to the United States. Now, in addition to traditional regional security issues, an array of “nontraditional” threats—including nuclear, chemical, and biological weapons proliferation; a hundred different varieties of terrorism; ethnic and religious conflict; organized crime; drug trafficking; and criminal anarchy—challenges U.S. well-being. These threats to U.S. national security are exacerbated by “nonmilitary” threats and menaces that have heretofore been ignored or wished away. They include trade war, financial war, new terror war (e.g., the improving sophistication of using nuclear, chemical, and biological weapons of mass destruction [WMD]), and cyber war. All these threats challenge the United States at home and abroad, and blur the conventional dividing lines between military, political, economic, and informational security affairs.

The combined effect of new, evolving, and increasing threats to U.S. national security is profound. It demands a new approach to both threat and response in terms of homeland defense. It suggests that, without significant changes in our national security thinking, structures, and processes, we face the grave risk that we will not be adequately prepared to deter and defend against traditional, nontraditional, and nonmilitary threats—and to minimize and contain the harm they might cause. The primary focus of our considerations and recommendations regarding these contemporary and future challenges is outlined below.

## The Historical Context for Dealing with Threats to the American Homeland.

A responsible, feasible, and achievable national security policy and strategy for the defense of the United States must begin with the values that we as a nation prize. In 1987, in observing the 200th anniversary of the United States Constitution, Americans celebrated these values with a sense of rededication—values such as human dignity, personal freedom, individual rights, ethical conduct, and the pursuit of happiness, peace, and prosperity. These are the values that lead us to seek a global order that encourages human rights, self-determination, the rule of law, legitimate institutions, economic prosperity, peaceful settlement of disputes, and the elimination of injustice. The ultimate purpose of U.S. national security policy and strategy is to protect and advance those values.

The Founding Fathers acknowledged that a viable government required a military establishment formidable enough to defend its citizens from outside threats, and any lawless elements that might develop in their midst. Nevertheless, they were extremely concerned about the possible abuse of power and the related threat to freedom represented by a standing army. As a result, the Founding Fathers relied heavily on the state militias, and tolerated a substantial standing military establishment only under the most extreme circumstances. Moreover, both the militias and the regular military forces of the United States were carefully circumscribed by the separation of powers and checks and balances enumerated in the United States Constitution.

At the same time, there was no constitutional requirement for the regular armed forces to provide support to civil authority. It is under the Common Law concept of “Necessity” that regular military support to civil authority has been allowed. In this context, military involvement in domestic affairs has been minimal, and the emphasis has been on the fact that the regular armed forces are always in



support of another federal, state, or local authority. Thus, the American military establishment has been on a short tether, and generally mandated to look outward—not inward.

Americans want to feel safe, but tend to be mistrustful of domestic law and order enforced by the regular military establishment, and—like their forefathers—are inclined to view military-type enforcement of federal authority as a serious threat to individual freedom and liberty. As a consequence, as American's leaders look for new and more effective ways to provide for the common defense and domestic well-being, the civilian and military contributors to this anthology agree that it would be wise to reconfirm the country's long-established values.

### The Complex Threat Situation.

Over the years, U.S. national security has generally been viewed as protection from external attack, and thought of largely in terms of military defenses against military threats. But, given the threats inherent in the predominantly interdependent global security environment, that is clearly too narrow a conception. American security today involves much more than the domestic procurement and external application of military forces. It includes important nonmilitary elements, as well as domestic and civil dimensions.

First, in the chaos of the “new world disorder,” the threat of devastating attacks on the United States, its interests, and its friends perpetrated by the former Soviet Union, China, or other contemporary nuclear powers retains a certain credibility. At the same time, the challenges to American security are expected to intensify with the growing sophistication of biological and chemical warfare. Third, these challenges are further complicated by traditional and nontraditional asymmetric threats emanating from virtually a thousand different state, intrastate, and transnational political actors with a

cause—and the will. Finally, the United States, its citizens, and its interests are severely challenged by nonmilitary threats by another thousand actors with access—as only one example—to cyber space.

Evidence of these threats is clearly seen in the North Korean capability to launch nuclear missiles that can reach the U.S. mainland; the Japanese *Aum Shinrikyo* cult's willingness to poison the Tokyo subway system; the foreign and domestic terrorist bombings of the New York City World Trade Center and the Oklahoma City Federal Building; some owners of international mobile capital willing to generate and exploit a financial crisis in Southeast Asia that inflicted social-economic-political devastation that could not have been exceeded by a regional war; and the very real amateur "hacker" or organized criminal capability to impair the security of an army or a nation electronically as effectively as a nuclear weapon.

The threat of any one or several political actors in the global community willing to use WMD, conventional weapons, and/or nonmilitary weapons for their own nefarious purposes is serious enough that it cannot be ignored. Moreover, the consequences—the aftermath—of contemporary warfare to the civil population and the national infrastructure are so serious that they must be addressed. In these terms, there is a clear requirement to prepare and plan more comprehensively for the civil-military implications of national defense. In the increasingly complex domestic security environment that is foreseen, the military establishment cannot deal with the diverse threats alone. Traditional military defense is but one element of a broader national security structure. If the United States is to be successful in meeting the threats—and the possible devastating consequences—of contemporary conflict and homeland defense now and in the future, it would seem reasonable to expect that the entire federal and state governmental structure become more cooperatively engaged.

## The Evolving Strategy and Structure for Homeland Defense.

For a long time—probably since the War of 1812—the continental United States has been relatively immune from the bloody consequences and physical destruction of conflict. As a result, the concept of homeland defense has been generally absent from American thinking. Recently, however, the issue of conflict and possible catastrophic consequences for the United States and its population is emerging in opinion polls as an important public concern.

The proliferation of information has provided the American public with several reasons for concern: (1) the experience of other members of the global community involved in bloody and horrible conflict; (2) the understanding that China, North Korea, and other nuclear powers are building intercontinental ballistic missiles that can reach the United States; (3) the perception of an enormous inventory of WMD—nuclear, biological, and chemical—ready to be used against American targets; (4) the reality of nontraditional and asymmetric warfare; (5) the emergence of transnational and intra-national nonstate actors not subject to deterrence through the classical military instruments of power; and, finally, (6) the realization that “it can happen here,” exacerbated by visions of confused, piecemeal, and ad hoc federal, state, and local responses to recent man-made and natural disasters that have taken place in the United States.

Thus, the lack of an evident policy, strategy, and structure for homeland defense has been validated by a congressional initiative asking the Department of Defense (DoD) to develop recommendations for a national strategy and organization to deal more adequately with the problem. Proposed solutions to the homeland defense issue include a DoD mandate for closer and more active involvement of the National Guard and other Reserve Components of the U.S. armed forces in the federal support to the homeland defense process—particularly in response to possible WMD

catastrophes. Proposed solutions to the problems of strategy (i.e., ends, ways, and means) and organization (i.e., defining who is in charge and how the various elements are integrated) have run-up against several "fault lines."

These obstacles are found between prevention and crisis management issues, and/or consequence management processes. As only a few examples, fault lines include: (1) the lack of a commonly accepted definition of homeland defense; (2) the generally reactive approach to law enforcement and national security matters that does not allow much latitude for proactive prevention or deterrence; (3) the lack of understanding concerning nontraditional and nonmilitary threats and how to deal with them; (4) crossing federal, state, and local jurisdictions; (5) interagency squabbling over appropriations, turf, and responsibilities at all levels of government; and, (6) the American citizen's right to privacy.

Despite the confusion, contributors agree that the message from the American people is clear. That is, if we want to preserve our domestic well-being and continue to benefit from it, we must take the necessary steps to defend it. Consensus is that the first step in an attempt to ensure the domestic tranquillity, and to manage the consequences of any possible attack on the homeland, would be the development of a new paradigm of cooperation. That, in turn, will require a historically viable and constitutionally supported unity of national effort. In these terms, military "command and control" must accommodate to "coordination and cooperation" in a federal system that includes separation of powers and checks and balances "to preserve the blessings of liberty." Another step within this transformation process would be the development of a broader concept of deterrence.

#### Some Critical Considerations and Recommendations.

Probably sooner than later, it is likely that the homeland defense issue will emerge "surprisingly" in the national

political arena. It is important that policymakers, decisionmakers, opinionmakers, other civilian and military leaders, and ordinary citizens are prepared to deal with this vital issue. In that connection, contributors made four critical arguments.

First, the temptation should be resisted to give the U.S. armed forces a mandate to “lead in support,” as a quick and easy solution to the complex federal, state, and civil liberties issues surrounding homeland defense. Several good reasons were set forth to support that argument. Suffice it to say here that we live in a conflictive and multicultural society in which there is a perception of some erosion of moral legitimacy in the Federal Government and its institutions. Thus, participants recommended that DoD do everything possible to pursue vigilantly a long-term strategy both to perform its primary war-fighting mission right and well, and to develop a better relationship with American society.

Second, rather than taking the easy way out of the problem, serious efforts should be made to develop a unified field theory for homeland defense. It will be difficult, but that theory will provide policy and strategy guidance, and will empower a new paradigm of federal, state, and local coordination and cooperation. Much like George Kennan did in developing the Cold War “containment” theory, contributors recommended that strategy “workshops” be conducted that will be instrumental in framing the philosophical underpinnings of an organizing theory to assist in clarifying basic objectives, courses of action, and the primary means for accomplishing those purposes.

Third, a vertical U.S. organizational architecture must be developed to facilitate the holistic implementation of carefully planned, direct and indirect, proactive and defensive political-diplomatic, social-economic, psychological-moral, and military-police measures against those who would violently or indirectly threaten the national security. The complexity of homeland defense in an interdependent global security environment also requires horizontal

cooperation between the United States and its external allies. Without both vertical and horizontal unity of effort, homeland defense measures may be irrelevant or even counter-productive. Thus, attendees recommended that strategy “workshops” be conducted that will in turn recommend legislative or other initiatives to create an organization at the highest level to establish, enforce, and continually refine an integrated national-global security policy and strategy.

Finally, within the parameters of a guiding theory for homeland defense and an integrating organizational architecture, it is important to develop a broader deterrence concept. The intent would be to supplement or replace the older and narrower nuclear deterrence paradigm with one that addresses the traditional, nontraditional, and nonmilitary threats imposed by the diverse state, nonstate, and transnational actors in the contemporary global and domestic security environments. Within the context of a field theory for homeland defense, the deterrence “rule of thumb” must move away from “rational” U.S.-held values. It must address the notion that there may be other “irrational” things that hostile elites might value. Moreover, it must accept the idea that other cultural “things” of value can realistically be held at risk. Conversely, a broader deterrence rule of thumb must also provide the basis for “carrots,” as well as “sticks,” to be offered as deterrents. An organizational understanding of motives, culture, and the ability to communicate, thus, becomes crucial to a new civil-military deterrence equation. Again, participants recommended that strategy “workshops” be conducted to craft a deterrence policy and strategy that addresses diverse contemporary security threats and responses.

## Conclusions.

Implementing the extraordinary challenges of reform and regeneration implied in these considerations and recommendations calls for a major paradigm shift. That will

not be easy. It will, however, be far less demanding and costly in political, monetary, and military terms than continuing a short-term and generally military approach to what is a long-term and multidimensional problem.

These challenges and tasks are nothing radical. They are only basic security strategy and national asset management. By accepting these challenges, decision-makers, policymakers, and opinionmakers can help fulfill the constitutional and moral mandate to provide for the defense of the American homeland, and fulfill the promise that the 11th Annual Strategy Conference offers.

# CHAPTER 1

## A STRATEGIC PERSPECTIVE ON U.S. HOMELAND DEFENSE: PROBLEM AND RESPONSE

John J. Hamre

I am going to speak as though I were still Deputy Secretary of Defense for one last hour, if I may, with the presumption that I can do that. But, first, I must tell you that I was amazed that you asked me to offer this keynote address, and it reminds me very much of a story that was once told of the great Lionel Barrymore, who was a famous Shakespearean actor at the turn of the century in England. Barrymore was playing the part of Richard II in the play *Richard II* by Shakespeare at the Old Vic in London. You know Richard was the hunchbacked, deformed bastard son of Henry. He was an ambitious man who decided to wage war against his father and his legitimate brother to take over the throne. And the story is about the warfare of Richard and his insurrection against Henry. In the second act of the play, the scene takes place on the battlefield and he's in a pavilion. A young page was supposed to run into the stage and say, "Sir, they have captured Glouster." Richard is to stand up and demonically laugh and say, "Take him out and have him hung." Well, this one night at the Old Vic there was a very young actor who was playing the role of this new squire, and he was so nervous that he was appearing on the stage with the great Barrymore. He was backstage rehearsing his line, "They've captured Glouster." He tried to get it right so that he could be perfect in timing and that sort of thing. At the crucial moment, he ran out on the stage, and he said, "Sir, they've captured Glouster and hung him." And then he just froze; he realized what he had done.

Of course he had cut off the great Barrymore. Time stopped. And Barrymore stared at this kid with a look that



would melt a rock. There was a pause that lasted for what seemed an infinity. Then, after the longest silence, Barrymore raised himself up and said, "Well, I'll be damned." So when former Commandant of the U.S. Army War College Major General Robert H. Scales, Jr., called me and said, "Even though you are no longer Deputy Secretary, I'd still like you to come and give a talk at this conference," I said, "Well, I'll be damned."

## Homeland Defense.

We are here to talk about homeland defense. Now this is a subject that has become quite current in the last several years. But frankly, it has been alien from American thinking for a very long time. Ever since the unpleasantness in 1814 when the British sailed up the Potomac and burned down the Capitol, we have not thought much about that. I remind people that it is quite an interesting new world we live in. We sing in our National Anthem, "And the rockets red glare, the bombs bursting in air." You know those were produced by Royal Ordnance, which is now a part of British Aerospace, our fifth largest defense contractor in the United States. So it is a very interesting new world we are living in.

But not really since 1812 or 1814 have we thought much about homeland defense. Now we have had some episodes where we have worried about it. During World War II, as you recall, if you were in California, there are still pictures that you can see of the dirigibles that were holding the steel cables up to provide a barrier against airplanes that might be attacking air fields. And if anybody is here from Boston, you probably remember that the gold dome, the Bullfinch Dome that is at the capitol of the Commonwealth of Massachusetts, was painted black at the outset of the war so it couldn't become a beacon for German bombers. But outside of a few specific and fairly limited instances, the United States has felt secure in its homeland for at least five generations. We really have not thought about it much.

## Reasons to Start Thinking about Homeland Defense Now.

Now it has come to be a matter of concern in the last 10 years. Certainly we are only starting to think about it intellectually in the last 2 or 3 years; it has become quite important to us. I think there are several reasons for that. First, the intellectuals in the defense establishment, all of you and your colleagues, have spent a fair amount of time talking about the asymmetric nature of warfare. When the United States is such a dominant force on the battlefield, especially conventionally, it is unlikely that another country will chose to do what Saddam did in 1990, which is to try to take on the United States or a coalition of Western powers in a conventional way. So we perceive that potential opponents would choose to confront us in a nontraditional manner. After all, why would a country like North Korea, which is a shattered country in all truth, go to the steps of building a 7,000-kilometers intercontinental ballistic missile (ICBM)? For what purpose, what plausible reason from a defense standpoint, would they need a missile that could reach 7,000 kilometers, if it were not to try to politically intimidate the United States? So we see this emergence of asymmetric threats where very small numbers of people can now wage war against the United States, at least in a political dimension. That is probably the first reason that we are focusing on it.

The second reason is that we are living with the residue of the Cold War. As the old Soviet Union broke up, it left an astounding inventory of bad things that are drifting into the hands of bad people—an enormous inventory of chemical, biological weapons and loose nukes. Just the other day there was a story of the Uzbeki border guards intercepting an illicit transfer of nuclear material. Equally, we are seeing the proliferation of knowledge. The huge infrastructure of knowledge that was built up in the old Soviet Union during the Cold War is now looking for employment and moving in directions that trouble us deeply.

The third thing is the emergence of a series of transnational actors like Osama bin Laden and his organization. These transnational actors do not seem to be susceptible to the classic instruments of deterrence. How do you deter an organization like Osama bin Laden's? So these things in combination have led to the United States thinking more creatively about the issues of homeland defense than at any time in the last 150 years.

We have a problem. First of all, I do not think we have a common understanding of what homeland defense really means. For some individuals, were we to take a poll, the first thing that would come to mind would be national missile defense, harkening back to Ronald Reagan's speech 15 years ago about national missile defense. That is what homeland defense means to a large number of members of Congress, for example. To others, it means defending the United States against threats by terrorist organizations using weapons of mass destruction (WMD), be they chemical or biological or nuclear. Yet to others, homeland defense means cyber defense, trying to protect America's infrastructure in an increasingly interconnected world. And there are others who think homeland defense is as basic as trying to stop the flow of illegal drugs into the United States.

## Two Cogent Issues in Homeland Defense.

Homeland defense means lots of different things to lots of people. One of the questions that we should come back to today is, "Is there a unified field theory for homeland defense?" I think that is an important question for us to talk about, especially for DoD to talk about. I think there are real problems about having a unified field theory for homeland defense, but we will talk about that later. I am not going to talk about the drug issue here. That is less my concern, not in a personal sense—obviously it is a great problem for the United States—but not for today's speech. I would like to talk about the first three meanings of homeland defense

noted above, and then come to the question at the end; that is, can we have a unified field theory for homeland defense?

First, let us examine the national missile defense issue. This, of course, is the one that is most familiar to a defense organization. It after all represents something that is most typical of a defense problem. We know how to operationalize the issue of homeland defense when it comes to missile protection. We can hypothesize a threat, operationalize it by putting time lines to an attack, characteristics to the nature of the attack, attack avenues or azimuth that we would have to worry about. We then could design a program to deal with that threat. This is a very classic military problem, with a very classic military solution. It is a matter of organizing resources to develop very sophisticated hardware, develop the command and control procedure, wire it together in reliable ways, work out the doctrine for its application, and so forth—a classic military problem. And it is one that engenders the least amount of confusion in the department when we think about it, not just because we have been thinking about it for 15 years, but because it is a classic military problem.

The second issue—that of WMD in the hands of terrorists—is inherently a much more complicated problem. First of all, it is not a purely military problem, even though it would on its face seem to be. There are two dimensions to this problem. One dimension is how do you stop the bad guys from doing something before hand? And then there is the second dimension; how do you cope with the consequences if we are not able to stop the terrorists, and what do we do as a defense department?

Let's take the first dimension. There are some very tough issues in this area of homeland defense. First, it gets to the core of some very serious fault lines that run up and down the American form of constitutional government, the fault lines between national defense and domestic security. After all, since 1873, when the *posse comitatus* law was put in place, DoD has been forbidden from undertaking law

enforcement actions inside the United States. *Posse comitatus* was narrowly defined at this start, as the lawyers here know. *Posse comitatus* really was passed because some members of Congress were fearful that the Federal Government was going to get involved in state politics in the South during the period of reconstruction after the Civil War. The law was passed to delimit the involvement of the Federal Government in state politics. But it has since transmogrified into an enshrined principle in American constitutional government where DoD does not do any civil law enforcement.

This is a very sharp fault line in the American form of government when it comes to the issue of WMD and the way that the government responds. Why? Well, if we postulate a significant terrorist event, a WMD-type event, we are dealing with an inherent limitation in local law enforcement. Law enforcement organizations are sized on a day-to-day basis for the normal load of crime and other problems in the neighborhood. They are not sized for the catastrophic event. There is no mobilizable capacity in local law enforcement organizations, other than to work overtime or borrow officers from a neighboring jurisdiction. I do not say this disparagingly. Local governments and state governments cannot afford and do not maintain mobilizable capability.

There is only one part of the government that maintains mobilizable resources, that are designed to be qualitatively different the day after an event compared to the day before. And that is DoD. We mobilize massive resources and put them into the field. That is what we do. And yet that is not what law enforcement lacks. This creates a very sharp friction point when it comes to a WMD event in the United States. How do we in DoD prepare for a catastrophic terrorist event like that when we have no authority to do so in peacetime? This is a very interesting problem.

There is a second problem fault line, and that is the fault line between our intelligence instruments as they relate to

threats outside of the United States and our intelligence instruments that relate to internal U.S. threats. As you know, DoD and its intelligence instruments are precluded from surveillance on any U.S. citizen. We are not allowed to undertake surveillance inside the United States, and we do not. That authority rests exclusively with law enforcement and especially with the Federal Bureau of Investigation (FBI). Similarly, the FBI lacks the capability to do things in a significant way outside of the United States.

We have this internal bureaucratic boundary as it were, with the border of the United States as it relates to the intelligence responsibilities. I saw this last December when we had very serious indications of a coordinated effort to detonate a device in the United States. We bumped up hard against this fault line on intelligence collaboration. Are we allowed to share information? Are we allowed to gather information? Under what authority are we allowed to do it? And when we examine cyber terrorism and cyber security, this becomes very problematic indeed. When you are talking about things that move at the speed of light and can move back and forth across that boundary at the speed of light, we have serious organizational problems.

There is a third fault line in this area, and that is inside DoD. As I said, we have two parts to the problem. The first part concerns stopping the bad guys before they can do something. The second part concerns dealing with the consequences after the fact. They take profoundly different skills. If you are trying to stop a terrorist organization before they have committed the act, DoD requires an organization of enormous agility, stealth, flexibility, and lethality. It takes special operations kinds of forces, forces that are able to quickly work in tight coordination with intelligence elements to locate the potential opponent.

But those critical skills are not helpful when it comes to dealing with the consequences after the fact. There you require an organization of transparency, public confidence, openness, massiveness, predictability. When you are

dealing with a society, you are dealing with a locality where literally thousands of people have potentially been exposed to an agent, when there is great panic in the community. It is not going to be the "snake eaters" that are going to be effective managers of that problem. I say that with affection and with enormous respect for the Special Operations people. These are very different sets of problems, and they require different organizational solutions. In sum, we have three fault lines that run up and down the government when it deals with this second area of homeland defense.

### How Do We Face These Issues?

The key question we now face is how do we tackle these issues. First, we have to find a solution to the way that the Federal Government is organized to deal with this problem. Part of our problem is that our entire federal response plan to emergencies at the local level revolves around the Federal Emergency Response Plan, which is run by the Federal Emergency Management Agency (FEMA). But FEMA has decided not to be actively involved in the issue of homeland defense. This is a serious problem. Everybody at the local level is used to looking to Washington with telescope lens, and they cannot see anybody at the other end. All of us in Washington are trying to communicate to the local levels through a different chain. We have a serious problem here. That is one of those problems that we have to solve.

How should the Federal Government organize to help local authorities? Because FEMA has not taken the lead, the Justice Department has stepped in. But as soon as this issue is channeled through law enforcement agencies, people on the ends of the spectrum get worried. On the right end, you find the "black helicopter" crowd that is all fearful that the Federal Government is going to come in and steal away their liberties. I do not understand this bunch, but we have a lot of them, especially west of the Mississippi. And east of the Mississippi, we have all of the leftist crowd. They watched the movie, *Siege*, one too many times, and they

have this fear that DoD just can hardly wait to come in and take over a city. Good grief. We in DoD have enough problems, let alone having to run Washington, DC. But nonetheless, the right and the left are paranoid about the Federal Government, and especially DoD, suspending civil liberties in time of emergency. So they do not even want us to prepare for catastrophic terrorism in peacetime.

Given these political realities, how do we organize the Federal Government to deal with homeland defense? Let me offer one point, and I say this with some passion. It reflects the arguments I have had on several occasions, especially with the American Civil Liberties Union (ACLU). The biggest threat to American civil liberties will come on the day that we have an event like this, and we have done nothing to get ready for it. If the only option available to the President is to declare martial law—to trigger the Insurrection Act and to declare martial law—that will be a tragedy in America that day. To avoid that terrible option, we must spend time now getting ready and tackle these tough problems.

There is a second issue we have to work on in this area, and that is the whole issue of federalism. We do not think about federalism much in the United States. Frankly, the people who do think most about it are the National Guard. I am referring to the relationship between the Federal Government and local government in dealing with a problem that transcends local political jurisdictions. This winter DoD undertook an exercise. We designed a stressful scenario in order to examine these issues. In this case scenario, a terrorist organization acquired a tactical nuclear device out of the old Soviet Union, brought it into the United States, and detonated it in a major metropolitan center. We conducted this exercise jointly with the Department of Justice and FBI to uncover some of these issues.

Let me share with you some of the problems we discovered. If the device goes off, the first reaction, of course, is the first responders rush to the site of the problem and



start doing what they can. During the first 2 hours, however, those first responders have used up their life-time supply of exposure to radiation. You've lost all your first responders in the first 2 hours. Second, how do you communicate to the 300,000 people that are within an hour's drive of the epicenter what to do? There is a plume of radioactive fallout that went downwind about 10 miles, and everybody who lives in that area is potentially exposed now to a dose of lethal radiation. Now the best thing for them to do is to stay in their basement for the next 24 hours. How do you find out on the ground where that plume went? How do you tell them? How do you become the one authoritative voice to tell people what to do? Every junior college physics professor in the country is going to be on the local television explaining what radiation is like. How do you establish the one voice that everybody listens to? Who is it? How do you tell a dad that he cannot drive into that area to pick up his kids in the day care center? And how are you going to stop him? These are tough issues.

Ultimately, these are federalism issues. At its core we are asking, "What is the legal authority in a geographical area in a time of an emergency of this magnitude?" Let me give you a very grim example. If there were such an event in this one scenario, we would have about around 48,000 radioactive human corpses in the area. What legal authority is needed to bury 48,000 radioactive individuals? Who has the authority? Currently, all legal authorities, of course, for burial are state and local. There are no federal authorities for burial. Does the President of the United States, for health and safety reasons, order the local National Guard to conduct open-trench burning? Who decides that? I know these sound terribly grim, but we have got to think our way through some of these issues. This is, by the way, what we call doctrine. We need to develop doctrine for consequence management.

At their core, these are federalism issues. Let me give you a very specific example. Do we federalize the National Guard? Of course, as soon as we do, we may not use them for

law enforcement because of *posse comitatus*. If the Guard remains under state authority, they may be used in law enforcement, but we now have split command and control. How are we going to work that out? We can find a solution, but we have to work it out in advance. This is developing the doctrine of consequence management, and we have to start working on it.

These are new problems to DoD. All war planning in DoD takes place in “CINCDoms” (combatant commanders’ areas of responsibility). Commanders in Chief (CINCs) do war planning. We do not do war planning in Service headquarters. We do not do it—and thank God we do not do it—in the Office of the Secretary of Defense. We do war planning in “CINCDoms.” The problem, of course, is that the United States has never been assigned to any CINC’s area of responsibility (AOR). I am excluding, of course, the Continental Air Defense mission. Aside from that, we have never put the United States into a CINC’s AOR. There are historical reasons for it, largely stemming from CINC and Service politics. The Services and the CINCs and the Chiefs wrestled with this problem recently when they developed the last Unified Command Plan. We could not get a consensus, again, in no small measure because of internal organizational politics.

There is also a larger question, which is this anxiety in the hearts of Americans, be they on the left or the right, of a military command over America. It fuels paranoia in people’s minds. For these reasons we have never assigned the United States to a CINC AOR. Of course, that means DoD has never developed war plans to defend the homeland. We have never developed training scenarios.

I think we have a temporary (and maybe long-term) solution when the Chairman and the Secretary recommended to the President that we create the Joint Task Force for Civil Support (JTF-CS). JTF-CS is working along with the Defense Threat Reduction Agency to come up with a series of operationalizing scenarios to try to define and

understand the nature of this problem, and to extract the lessons that we have to learn so that we can develop a new doctrine for homeland defense. That is why this conference is so important. We must assemble creative minds to think through such hard problems as this. So I commend you for holding this conference.

### The Third Issue of Homeland Defense.

The third issue of homeland defense is cyber protection. This is quite different, of course, from the national missile defense and from the WMD terrorism categories. First, there is a definitional problem. How and when do you know when this is a national security issue as opposed to a law enforcement issue? At what point is it ever clear that this is an act of war? Second, the infrastructure that is under attack is civilian, not military. A cyber attack is likely to be entirely against private sector infrastructure. For example, even DOD's command and control system is largely in the private sector. We no longer have big, complex, wholly-owned telephone switches and dedicated communication facilities. Now we contract for this from the private sector. So a cyber attack is most likely going to fall on the private infrastructure of the United States. And, frankly, they do not think this is a problem right now. Some companies have had problems, and they want to keep it very quiet. The last thing a Wall Street investment banker wants to acknowledge is that they have been hacked, for fear that the event will create bad publicity that might affect the company's financial standing. The private sector is not going to want to advertise that they just have had a problem. So how do we, the Federal Government, provide homeland defense in cyber space to a community that does not feel they need our help? You certainly cannot do it by federal mandate.

I believe we have to develop a very different approach for cyber security. We have to find a method that provides incentives for the private sector to want to find protection

for itself, rather than to mandate it. I think we need to find ways to create either tax incentives or indemnification incentives for companies that invest in protective infrastructure. So, for example, if a company invests in a virtual private network with encryption around its infrastructure, maybe its insurance company will give it a break on its insurance rates. In this instance the role for us, the Federal Government, is to delimit the liabilities of the corporations and the insurance companies through some sort of a secondary market. I think that is how we are going to have to fix the problem of protecting America's infrastructure in cyber space. It is not a classic military problem. So in this instance, ironically, homeland defense in cyber space probably means working through the Ways and Means Committee, not through the Armed Services Committee.

What is the appropriate role for the Federal Government, and especially for the defense establishment, when it comes to cyber space protection? My personal feeling is that, in this area, our role is probably one that deals with providing intelligence and surveillance of cyber space and providing that information reliably to people in the United States, be it to law enforcement or to private sector entities.

Here again, we confront the very difficult problem of what is the Federal Government's role regarding surveillance on U.S. citizens. It is very hard to distinguish in cyber space when a bad guy all of a sudden becomes an American citizen. As soon as we find that any of our surveillance activities overseas connects to an American citizen, we have to turn off surveillance in order to protect their privacy. This is a serious problem. We need to find ways to link the lawful authorities that exist for surveillance inside the United States and the authorities and responsibilities that we have for overseas intelligence. But this raises many difficult problems which we need to address.

## Conclusions.

Now let me wrap this up with a concluding observation. Is it possible to develop a unified field theory for homeland defense? I am dubious because of the very different nature of these three homeland defense problems. National missile defense is a classic military problem. WMD terrorism is a hybrid problem, especially in the area of consequence management. Here the problems are federalism issues, not exclusively or even largely in the jurisdiction of DoD. Finally, for cyber security issues, virtually none of it rests with the Federal Government. So, is it possible to develop a unified theory for homeland defense? I doubt it, because it will be extremely difficult. That does not mean we should not try to develop a unifying paradigm as the federal and state governments work through and think about all of these problems.

Right now, however, the most important thing was for us to create the Joint Task Force for Civil Support (CTF-CS). The CTF-CS only deals with the WMD terrorist incident. It is not dealing with the National Missile Defense (NMD) problem, and is not dealing with the cyber problem. Those two problems are assigned to the Space Command. I think it is still an open question as to how successful we will be by putting cyber protection at Space Command. But that is another issue for another day.

Ultimately, there is only one CINCUSA, and that is the President as the Commander in Chief. We have got to provide him the reliable staffing structure so that he can be effective in that role.

So what do we need to do, and what am I asking you to do? First, I think we need to properly define the homeland defense mission. Second, we need to develop military doctrine for these problems. That has to be grounded in the operationalization of the threat. I think some of that work is underway, work that needs to be done on the basis of exercise but grounded with a good theoretical underpinning

that a theory for homeland defense could be possible. That is what you should be doing at this conference. Third, I think we need disciplined thinking—a new paradigm of cooperation—on the tough federalism issues. How do the Federal Government and the state and local governments work together at times of extraordinary crisis? We know how to cooperate when there are natural disasters. We do not seem to know how to cooperate if there is a catastrophic terrorist incident. Finally, we in DoD have to figure out how we support law enforcement as the junior partners in the enterprise. DoD must act in a subordinate role to others who do have it as their primary responsibility to provide homeland defense.

It is absolutely crucial that you are holding this conference. I do not know when you made plans for this conference, but I am very grateful that you did. We are running on borrowed time. I think it is just a matter of time before we have an event in this country that will be absolutely the most stressful thing to confront the country since the War of 1812. We cannot afford not to be ready for it, because at that moment everybody in the country is going to be looking for their government to respond with competence and assurance.

We will either frighten them, or we will reassure them that we will get through it, depending on our preparations. This conference is the starting point. I hope that many of you in your respective organizations will see this as your responsibility to take this even further as we work through these issues. I thank you for the opportunity to be with you today.

## CHAPTER 2

### THE ARMY OF THE CONSTITUTION: THE HISTORICAL CONTEXT

Gregory J. W. Urwin

Everyone who enlists in the United States Army is required to take the following oath:

I do solemnly swear (or affirm) that I will support the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same.<sup>1</sup>

In other words, American soldiers are expected to lay down their lives for a piece of paper, but that is not as absurd as it sounds. For the Constitution exists to serve a high purpose, as its framers took pains to explain in their Preamble—"to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty." That definition of good government contains a decidedly military thrust. Governments usually provide for their defense by maintaining armed forces, and those forces are sometimes called upon to keep order at home.<sup>2</sup>

Yet while the men who drafted and ratified the Constitution might have agreed on the general purpose of government, they clashed over the proper means for ensuring national security. The years in which the United States won its independence and became a viable nation also witnessed a drawn-out and prickly debate over military policy. Americans argued about how much military power they were willing to entrust to the national government, as well as when and against whom that power should be employed.<sup>3</sup>

Although anti-militarism permeated the basic political philosophy of the Founding Fathers, they could not escape the fact that theirs was a nation born in war. The more realistic among them acknowledged that the general welfare and blessings of liberty could not be safeguarded without occasional resort to arms. Despite ideological disputes and increasingly bitter partisanship, they managed to construct a military system that would govern America's responses to its enemies, both foreign and domestic, for a century following George Washington's presidency. That system, and the assumptions that supported it, continue to influence our current defense establishment. As America's leaders search for new ways to serve the republic's security interests in an age of uncertainty, they would do well to revisit the country's military roots.<sup>4</sup>

The English adventurers, businessmen, and religious zealots who established the Thirteen Colonies encountered a variety of military threats—Indians, Spaniards, Frenchmen, Hollanders, and pirates—in the New World. England possessed no standing army when the great migration began in earnest in the early 17th century. Even if the colonizing bands who crossed the Atlantic had been inclined to import that relatively new European institution, they lacked the financial resources to support a substantial number of full-time soldiers. Thus, those vulnerable communities attempted to meet their military needs with a less costly defense system—a system that was well into decline in the mother country—the militia.<sup>5</sup>

The militia, which traced its origins to Saxon England, rested on the principle of universal military service. All of the Thirteen Colonies, except for Quaker Pennsylvania, passed legislation that turned their adult male inhabitants into part-time soldiers. Each man aged 16 to 60 was expected to own a modern weapon, train regularly with his neighbors, and stand ready to repel any attack on his colony.<sup>6</sup>



As the colonies expanded and prospered, however, the militia system grew weaker rather than stronger. Socio-economic concerns figured prominently in that decline. The cost of acquiring a sound musket, sufficient powder and shot, and a suitable edged weapon eventually transformed the militia into the exclusive province of white, propertied males. Slaves, free blacks, indentured servants, apprentices, drifters, and Indians were weeded out of the ranks in the name of order and internal security. At the same time, colonial authorities came to feel that calling out large numbers of solid citizens in response to every military crisis was both politically risky and economically disruptive—especially as those emergencies normally occurred on the distant frontier. Nevertheless, the militia lived on as a middle-class association chiefly concerned with protecting property and the local status quo. It schooled young men in elementary military science, restored law and order in unruly districts, and guarded against slave revolts, but it ceased to be the only means of colonial defense long before the American Revolution.<sup>7</sup>

In place of the militia, colonial governments took to guarding their frontiers with paid troops raised for set periods of time—ordinarily a campaign season or a full year. These semi-regulars came to be known as “Provincials.” Ideally, Provincial units were to fill their ranks with voluntary enlistments or draftees from the militia, but the latter expedient met with increasing resistance. Eventually, many of the men who joined the Provincials turned out to be the very ones barred from militia service—the poor and propertyless. This marked the start of a recruitment pattern that would persist to the present time. America has often entrusted its defense to those who enjoy the smallest shares of its bounty.<sup>8</sup>

During the Seven Years’ War, Great Britain finally sent enough regular regiments to North America to eliminate the French threat to the Thirteen Colonies. Despite the Redcoats’ heroic achievements and the colonies’ heavy reliance on semi-regulars, 18th century Americans

exhibited a strong antipathy toward the notion of standing armies. Steeped in the history of ancient Greece and Rome, Americans believed that a military establishment without a war to keep it occupied would inevitably turn against the people it was supposed to protect. The more recent excesses attributed to Oliver Cromwell and James II helped inspire the radical Whig ideology that the colonists imbibed from their English cousins.<sup>9</sup>

These words, published under a pseudonym in 1788, summed up what had long been an entrenched attitude in American society:

It has ever been held that standing armies in times of peace are dangerous to a free country; and no observation seems to contain more reason in it. Besides being useless, as having no object of employment, they are inconvenient and expensive. The soldiery, who are generally composed of the dregs of the people, when disbanded, or unfit for military service, being equally unfit for any other employment, become extremely burthensome. . . . The severity of discipline necessary to be observed reduces them to a degree of slavery; the unconditional submission to the commands of their superiors, to which they are bound, renders them the fit instruments of tyranny and oppression.— Hence they have in all ages afforded striking examples of contributing, more or less, to enslave mankind.<sup>10</sup>

The decade preceding the American Revolution intensified this hostility to a virulent degree. By dispatching regular regiments to Boston in 1768-69 and 1774 to intimidate the contentious Massachusetts Whigs, Great Britain only succeeded in causing many colonists to regard Redcoats as the ultimate symbol of military despotism. As an open break approached, those opposing Parliament's efforts to curb colonial autonomy transformed the militia into a potent political tool. They ousted Loyalist officers and had a revolutionized militia prod the populace into backing the resistance movement.<sup>11</sup>

The New England militia proved its willingness to fight on April 19, 1775, when it engaged in running battle with

1,700 British regulars from Concord to Boston, Massachusetts. Having started a full-fledged war, New Englanders looked to the Middle and Southern Colonies for assistance. The Massachusetts assembly invited the Second Continental Congress to assume responsibility for the 10,000 to 20,000 angry Yankees who were keeping 4,000 Redcoats penned in Boston. Congress complied on June 14, 1775, designating that hastily assembled and irregularly governed force "the American continental army."<sup>12</sup>

The military system first adopted by the Continental Congress resembled its colonial predecessors. Like Provincials, Continental soldiers were initially enlisted 1 year at a time, but the wisdom of that arrangement came into question as the course of the war turned against the rebels. The fall of New York City and the near disintegration of the Continental Army in the latter half of 1776 demonstrated that the survival of the infant United States required an army of long-term regulars. On September 16, 1776, Congress voted to obligate Continentals "to serve during the present war." Aware that the majority of Americans would not consent to put their personal interests on hold for the duration of a long war, Congress instituted a recruitment policy that deliberately appealed to the down and out. Enlistees were promised \$20 bounties (later raised to \$80) and 100-acre land grants. Consequently, the Continental Army drew the bulk of its strength from the lower echelons of American society—vagrants, loafers, the unemployed, indentured servants, debtors, free blacks, and slaves. Some recruiters even signed up enemy deserters, prisoners of war, ordinary criminals, and Tories sentenced to death.<sup>13</sup>

Despite these economic inducements, the Continental Army's actual strength never neared authorized levels. General George Washington and other Continental commanders did not dare to give battle without calling out a sizable increment of militia to back up their undermanned regulars. For its part, the militia compiled a mixed combat record during the War for Independence. It stood fast at

times, as at Breed's Hill, Bennington, Oriskany, and Cowpens. On other occasions, it broke and ran at the slightest pretext. Given such unpredictable conduct, it is no wonder that most senior Continental officers expressed a low opinion of the militia.<sup>14</sup>

Militiamen may have had their limitations, but they made indispensable contributions to the winning of independence in their familiar role of home defense. They suppressed local Loyalists, patrolled the coastline, guarded frontier settlements, and protected the countryside from enemy foragers and raiders. Along with the Continental Army, the militia prevented the British from reestablishing royal authority anywhere except for a few restricted enclaves. The British did not have enough troops available to occupy the Thirteen Colonies in force. If they spread themselves too thin, the Patriots could defeat them in detail, which is what happened at Trenton, Princeton, Saratoga, and Yorktown. The Patriots lost more battles than they won, but they persevered in a war of attrition that sapped British resolve and secured American independence.<sup>15</sup>

When the War for Independence erupted, the Thirteen Colonies possessed no central government. The Second Continental Congress, which convened at Philadelphia in May 1775, took on that role by default. After all, it was the only pan-colonial body in existence and had been formed to coordinate resistance to British policies. Managing a protest movement that had escalated into armed revolt turned out to be the next logical step.<sup>16</sup>

Exhibiting the same legalistic bent as the English enemy, Congress sought to legitimize its position with a written constitution called the Articles of Confederation. The task of writing this document fell to the multi-talented John Dickinson of Pennsylvania. Congress received his draft on July 12, 1776. It was Dickinson who coined the phrase "for the common Defence, or general Welfare." He selected those words to define the financial obligation that

the states owed to the Confederation. To put it plainly, any expenses incurred on behalf of the Continental Army or Navy, which acted in defense of all the states, were to be paid “out of a common Treasury.”<sup>17</sup>

The final version of the Articles, which was not ratified until 1781, retained Dickinson’s formulation of the common defense. For the most part, Congress had “the sole and exclusive right and power” to wage war and make peace, but individual states were permitted to defend themselves against imminent attacks and actual invasions. Article IX endowed Congress with the authority to

build and equip a navy—to agree upon the number of land forces, and to make requisitions from each state for its quota, in proportion to the number of white inhabitants in such state.

Except for small garrisons at a few frontier or coastal forts, no state could maintain standing forces in peacetime. Nevertheless, each state was to

keep up a well regulated militia, sufficiently armed and accoutred, and shall provide and constantly have ready for use . . . a due number of field pieces and tents, and a proper quantity of arms, ammunition, and camp equipage.<sup>18</sup>

Essentially, the Articles of Confederation formalized the loose-knit alliance that the rebellious colonies cobbled together to improve their chances of throwing off British rule. This was a marriage of convenience, and any state felt free to disregard its provisions whenever they became inconvenient. Congress lacked the power to force a state to do anything against its will. Consequently, requisitions for troops and money met with either partial or total noncompliance. With the end of the Revolution and the elimination of a direct British threat, the states found even less reason to cooperate with Congress or each other. This situation seriously hampered the Confederation’s ability to provide for the common defense.<sup>19</sup>

Once it became evident that the Yorktown defeat had undermined Britain's will to continue the war, pressure built in Congress to reduce the Continental Army. There was even some doubt that the Articles entitled Congress to maintain an army and navy after the cessation of hostilities. The mutinies that swept the Pennsylvania and New Jersey Lines in early 1781, plus the abortive attempt 2 years later by some Continental army officers to organize a military coup at the Newburgh Cantonment, lent fresh confirmation to the long-standing suspicion of standing armies. On April 23, 1783, Congress instructed Washington to furlough as many Continentals as he saw fit. By October 18, the Continental Army had shrunk to a single regiment of 600 men under Colonel Henry Jackson.<sup>20</sup>

Certain congressmen harbored reservations about such precipitate disarmament. Among them was Alexander Hamilton of New York, a former member of Washington's staff and a genuine combat hero. As chairman of the committee appointed on April 4, 1783, to examine the future conduct of the Confederation's foreign, Indian, and military affairs, Hamilton solicited Washington's guidance on the proper size and structure of a peacetime military force.<sup>21</sup>

Washington responded in less than a month with his famous "Sentiments on a Peace Establishment." Washington recommended the creation of "a regular and standing force" of 2,631 officers and men to garrison West Point and enough frontier posts "to awe the Indians, protect our Trade," and prevent encroachments on American territory by the British in Canada and the Spanish in the Floridas and Louisiana. Hoping to allay his countrymen's prejudices, Washington asserted:

'Altho' a large standing Army in time of Peace hath ever been considered dangerous to the liberties of a Country, yet a few Troops, under certain circumstances, are not only safe, but indispensably necessary.

He also demonstrated his political acuity by saluting the militia as “this great Bulwark of our Liberties and independence.” To make those words a reality, Washington favored militia reform. He proposed that militiamen be classed by age, with younger men between 18 and 25 obliged to train longer and respond first to military emergencies.<sup>22</sup>

Enlarging on Washington’s recommendations, Hamilton pushed for 3,000 regulars backed by an elite citizens’ volunteer corps. The latter was to be recruited from the cities for 8-year hitches, and armed, clothed, and paid by the central government. As fate would have it, Congress accepted neither plan. On June 2, 1784, it discharged all of Jackson’s regiment except for 80 privates to guard military stores at West Point and Fort Pitt. With this, the Continental Army passed into history.<sup>23</sup>

The day after Congress disbanded the last of the Continental Army, it created what historian Richard H. Kohn has called “the first peacetime military force in American history”—a single regiment consisting of 700 men drawn from the militias of Pennsylvania, Connecticut, New York, and New Jersey to serve for a maximum of 12 months. This 1st American Regiment, as it was to be known, was more a constabulary than an army, its ten companies split up into small detachments to furnish a token military presence along the Ohio Valley. Kohn characterized it as

a compromise force: not under state control, and enlisted for service out-of-state; not wholly under Confederation authority, not long-service regulars, and furnished obviously at the pleasure of the states, so certainly not a standing army. The Confederation’s “army” was unique, undefinable, and . . . the bastard child of quarrelsome, uncertain congressional parents.<sup>24</sup>

On April 12, 1785, Congress converted the 1st American Regiment into a regular corps by lengthening enlistment terms from 1 to 3 years. Regardless of this minor breakthrough, chronic desertion and a paucity of willing recruits kept the regiment’s numbers well below authorized

strength. Undeterred by this feeble frontier guardian, Indian raiders crossed the Ohio River at will, murdering 1,500 Kentucky settlers between 1783 and 1790.<sup>25</sup>

As if these Indian depredations were not bad enough, America's domestic tranquility was soon threatened by the specter of popular unrest. In the decade before the War for Independence, colonial elites repeatedly incited the lower classes to take to the streets to forcibly halt the execution of objectionable British laws. Once independence was won, however, patrician Patriots expected the common folk to abstain from mob violence—but old habits died hard. In the fall of 1786, Daniel Shays, a former Continental captain, led a revolt of debtor farmers that convulsed western Massachusetts. Dispersed impotently along the fringes of the Old Northwest, the 1st American Regiment was in no position to suppress domestic turmoil in the country's more settled areas. Massachusetts eventually fielded enough loyal militia to rout the Shaysites on January 25, 1787, in a clash at Springfield that claimed the lives of four rebels.<sup>26</sup>

Although Shays' Rebellion was completely crushed by March, it produced psychological tremors that shook the United States from one end to the other. Disillusioned by the Confederation's weaknesses and the rising spirit of unrestrained democracy, prominent Americans pointed to the fact that the disturbances had lasted for more than half a year, and Congress had done nothing tangible to suppress them. No one was more unnerved by these events than George Washington, who feared that the trouble in Massachusetts would spawn uprisings in other states. "I feel . . . infinitely more than I can express to you, for the disorders which have arisen in these states," Washington confided to Henry Knox, one of his most trusted subordinates from Continental Army days.

Good God! . . . Notwithstanding the boasted virtue of America, we are far gone in everything ignoble & bad. . . . It is scarcely within the reach of human ken, at this moment, to say



when—where—or how it will end. There are combustibles in every State, which a spark may set fire to. . . .<sup>27</sup>

In Washington's eyes, mob rule endangered the very future of the American experiment in self-government:

It is with the deepest, and most heart felt concern, I perceive . . . that the Insurgents of Massachusetts . . . are still acting in open violation of Law & Government. . . . What, gracious God, is man! It is but the other day we were shedding our blood to obtain Constitutions under which we now live—Constitutions of our own choice and framing—and now we are unsheathing the Sword to overturn them! The thing is so unaccountable that I hardly know how to realize it, or to persuade myself that I am not under the visions of a dream.<sup>28</sup>

According to Washington, "the thinking part of the people of this Country" concurred with the conclusion that he drew from Shays' Rebellion: "These disorders are evident marks of a defective government." Bowing to the mounting demand, Congress acquiesced to calls that a convention meet in Philadelphia to revise the Articles of Confederation. Twelve of the thirteen states sent delegates to participate in these deliberations. As part of the Virginia delegation, Washington traveled north determined "to adopt a more vigorous and energetic government, than the one under which we now live."<sup>29</sup>

Of the 55 delegates who assembled at Philadelphia between May and July 1787, 30 had seen some soldiering in the Revolutionary War—17 with the Continental Army and 13 in the militia. Not surprisingly, military affairs loomed large among their concerns. When the convention opened its formal sessions on May 29, a Continental veteran, Governor Edmund Jennings Randolph of Virginia, took the floor to denounce the defects in the Articles of Confederation in terms of national defense. Randolph claimed that "the confederation produced no security agai[nst] foreign invasions," could not prevent the states or individual Americans from starting wars, and lacked the authority and financial means to wage war itself. Congress could not even

"check quarrels between states, nor a rebellion in any," as it had no right to send troops into any state without the latter's invitation.<sup>30</sup>

Having sketched this portrait of congressional helplessness, Randolph boldly urged that the convention create a stronger constitution to replace the Articles and actually "accomplish the objects proposed by their institution; namely 'common defence, security of liberty and general welfare.'" By accepting Randolph's resolution, the gathering at Philadelphia transformed itself into the Constitutional Convention, and its members would go down in history as the Founding Fathers.<sup>31</sup>

In general terms, the Founding Fathers believed that a stable government required a military capacity formidable enough to shield its citizens from outside threats and any lawless elements that might spring up in their midst. As George Washington attested: "Vain it is to look for respect from a broad, or tranquillity at home . . . till the wisdom and force of the Union can be more concentrated and better applied." Alexander Hamilton of New York agreed with his former commander. "A certain portion of military force," Hamilton stated, "is absolutely necessary in large communities." William Paterson of New Jersey observed that "no government could be energetic on paper only," adding "there must be a small standing force to give every government weight."<sup>32</sup>

Although the majority of the Founding Fathers had outgrown the common taboo against standing armies, that did not make them militarists. They wanted to set up a national government that drew its authority from the consent of the governed, and not a line of bayonets. As Virginia's George Mason reminded his fellow delegates: "You can no more execute civil Regulations by Military Force than you can unite opposite Elements, than you can mingle Fire with Water."<sup>33</sup>

By mid-September, the Constitutional Convention had reached agreement over a compact that prescribed a

national government with definite military powers. The final version of the Constitution permitted Congress to declare war, commission privateers, raise and support armies, build and maintain a navy, and approve all regulations necessary to govern the armed forces. Still obsessed with the lingering trauma of Shay's Rebellion, the delegates transferred considerable authority over the militia from the states to Congress:

To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections, and repel Invasions;

To provide for organizing, arming, and disciplining the Militia, and for governing such Part of them as may be employed in the Service of the United States, reserving to the States respectively, the Appointment of the Officers, and the Authority of training the Militia according to the discipline prescribed by Congress.<sup>34</sup>

The Constitution established a single executive and endowed that position with military prerogatives befitting one of Europe's royal heads of state: "The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States."<sup>35</sup>

Such striking breaks with the past were not effected without a certain amount of wrangling. Elbridge Gerry of Massachusetts, the inveterate foe of standing armies and national military power, tried to insert a clause that would restrict Congress to raising a maximum of 2,000 to 3,000 regulars in peacetime. As for entitling Congress to federalize the militia to subdue revolts, Gerry huffed that he could not countenance "letting loose the myrmidons of the U. States on a State without its own consent."<sup>36</sup>

On August 18, George Mason of Virginia set the stage for the convention's liveliest debate on military affairs when he moved that Congress oversee "the regulation and discipline of the Militia of the several States reserving to the States the appointment of the Officers." Mason argued that a

revitalized militia would lessen the republic's need for a standing army in peace aside from a few regular garrisons on the frontier. A committee of 11 delegates took Mason's idea and refashioned it into a clause that enabled Congress "to make laws for organizing, arming & disciplining the Militia."<sup>37</sup>

When the Committee of Eleven reported its "Militia Clause" to the convention on August 23, the body language and facial expressions of certain delegates registered their displeasure. Rufus King, a member of the committee who had also battled the British as an officer in the Massachusetts militia, tried to defuse controversy. By organizing, arming, and disciplining the militia, King explained, the committee meant only that Congress would set the tables of organization to be followed by militia units, standardize the weapons types they could carry, and choose the manuals under which they would train. An unmollified Gerry shot back that he would as soon see

the Citizens of Massachusetts . . . disarmed, as to take the command [of the militia] from the States, and subject them to the Genl Legislature [Congress]. It would be regarded as a system of Despotism.<sup>38</sup>

Though Gerry and a handful of other delegates retained their misgivings, the majority seemed to feel that the Constitution contained sufficient safeguards to prevent the rise of an American Caesar or Cromwell. No congressman could hold any other federal post during his term of office, including a commission in the regular army or navy. A civilian President would nominate the heads of executive departments and higher ranking military officers, but his choices had to be approved by the Senate. Military appropriations could only cover 2-year periods, which allowed the House of Representatives to shrink or eliminate any federal forces that outlived their usefulness. Dismissing the fear that a federalized militia might be used to subjugate the states, Edmund Randolph pointed out: "Leaving the appointment of [militia] officers to the States

protects the people agst. every apprehension that could produce murmur." The convention demonstrated its sensitivity to this issue a second time when it voted down James Madison's motion that the national government name militia generals.<sup>39</sup>

On September 17, 1787, 38 delegates and the convention's secretary signed the Constitution. Another delegate, John Dickinson, was too ill to be present at Independence Hall that day, but he had a colleague affix his signature. Twenty-three of the signing delegates were Revolutionary War veterans, as was their secretary, William Jackson. The publication of the Constitution in October created a sensation in the republic. Nine months would elapse before 11 of the 13 states ratified it. During that time, the Constitution's merits were roundly debated from Massachusetts to Georgia.<sup>40</sup>

Anti-Federalists, as opponents of the Constitution were labeled, disliked the new frame of government for several reasons—not the least of which were its military provisions. In most instances, their objections pertained to the possibility that regular troops would be raised while the republic was at peace. A wave of speeches, pamphlets, and newspaper articles resurrected the same hoary diatribes that had inflamed the indignant passions of thousands of Americans a generation earlier.<sup>41</sup>

Addressing readers of the *New York Journal* "A Son of Liberty" cataloged "*a few of the curses*" that "this preposterous and new-fangled system" would impose on the United States. At the top of the list, he put:

1st. A Standing army, that bane to freedom, and support of tyrants, and their pampered minions; by which almost all the nations of Europe and Asia, have been enslaved.

A common Anti-Federalist scenario held that the standing army's main duty would be collecting the oppressive taxes required to sustain an enlarged national government. If state authorities protested, they would be stripped of their

powers at bayonet point. If the people dared to voice their discontent, the regulars would gun them down.<sup>42</sup>

Writing under the alias of "Agrippa," James Winthrop cautioned readers of the *Massachusetts Gazette*:

We shall find it impossible to please two masters. In such a state frequent broils will ensue. Advantage will be taken of a popular commotion, and even the venerable forms of the state be done away, while the new system will be enforced in its utmost rigour by an army. I am the more apprehensive of a standing army, on account of a clause in the new constitution which empowers Congress to keep one at all times; but this constitution is evidently such that it cannot stand any considerable time without an army.<sup>43</sup>

In a speech before the Virginia State Ratifying Convention in Richmond, the celebrated Patrick Henry thundered that the Constitution would subject Americans to the same sort of oppression that allegedly prevailed in Great Britain:

You read of a riot act in a country which is called one of the freest in the world, where a few neighbours cannot assemble without the risk of being shot by a hired soldiery, the engines of despotism. We may see such an act in America. A standing army we shall have also, to execute the execrable commands of tyranny: And how are you to punish them? Will you order them to be punished? Who shall obey these orders? Will your Mace-bearer be a match for a disciplined regiment?<sup>44</sup>

Luther Martin of Maryland, a disaffected member of the Constitutional Convention, warned that an ambitious President could use his military powers to burden America with a monarchy:

That the army and navy, which may be increased without restraint as to numbers, the officers of which, from the highest to the lowest, are all to be appointed by him, and dependent on his will and pleasure, and commanded by him in person, will, of course, be subservient to his wishes, and ready to execute his commands; in addition to which, the militia also are entirely subjected to his orders. That these circumstances, combined

together, will enable him, when he pleases, to become a king in name, as well as in substance, and establish himself in office not only for his own life, but even, if he chooses, to have that authority perpetuated to his family.<sup>45</sup>

A Massachusetts gentleman informed the *Connecticut Journal* that he saw no real safeguard in the Constitution's 2-year limit on military appropriations: "A great deal of mischief may be done in two years, with *guns, swords, and bayonets*, and armies when once raised, it hath some times been found difficult to disband."<sup>46</sup>

Turning to the claim that regulars were essential for national defense, the Anti-Federalists countered that the sort of men recruited by standing armies could not be counted on to withstand the terrors of battle. In a Philadelphia paper, the *Independent Gazette*, "John Humble" declared that an American standing army would be "composed of the purgings of the jails of Great Britain, Ireland and Germany." A commentator calling himself "Philadelphiensis" published this dire prediction in Philadelphia's *Independent Gazetteer*:

And in respect to the *standing army*, it will only be made up of profligate idle ruffians, whose prowess will chiefly consist in feats of cruelty exercised on their innocent fellow citizens; but in facing a foreign foe, they will prove themselves to be a body of mean cowards; like the Turkish Janissaries, better acquainted with plundering their country than fighting for its protection.<sup>47</sup>

This outpouring of anti-militarism did not signify that the Anti-Federalists had embraced pacifism. They simply believed that the United States should entrust its safety to the militia, which a pamphleteer posing as "A Columbian Patriot" exalted as "the bulwark of defence, and the security of national liberty."<sup>48</sup> Conveniently forgetting the Continental Army's part in winning the Revolution, "A Democratic Federalist" expostulated in the *Pennsylvania Herald*:

Had we a standing army, when the British invaded our peaceful shores? Was it a standing army that gained the battles of Lexington, and Bunker's Hill, and took the ill fated Burgoyne? Is not a well regulated *militia* sufficient for every purpose of internal defence? And which of you, my fellow citizens, is afraid of any invasion from foreign powers, that our brave militia would not be able to immediately repel?<sup>49</sup>

James Monroe of Virginia, though a Continental veteran himself, urged the future national government to avoid the problems associated with standing armies by reforming the militia:

Let them [Congress] regulate the disciplining and training of the militia—the calling them forth and commanding them in service; for the militia of a country is its only safe and proper defence. All countries are more or less exposed to danger, either from insurrection or invasion and the greater the authority of Congress over this respectable body of men, in whose hands every thing would be safe, the less necessity there would be, to have recourse to that bane of all societies, the destroyer of the rights of men, a standing army.<sup>50</sup>

In this instance, however, Monroe was something of an exception. Many more Anti-Federalists bridled at the notion of giving the national government any supervisory power over the militia. "By organizing the Militia," ranted Luther Martin, "Congress have taken the whole power from the State Governments." A Massachusetts critic viewed the provision for calling the militia into national service as a poorly disguised mechanism for creating military tyranny. "It means," he explained, "to convert the militia of the states into a standing army, under the entire command and control of Congress." "A Son of Liberty" tried to arouse opposition to a federalized militia by appealing to deep-seated American provincialism:

The militia of New Hampshire, or Massachusetts, dragged to Georgia or South-Carolina to assist in quelling an insurrection of Negroes in those states; and those of Georgia, to another distant quarter, to subdue their fellow citizens, who dare to rise against the despotism of government.<sup>51</sup>



The most comprehensive defense of the Constitution's "Army" and "Militia" clauses flowed from the facile pen of Alexander Hamilton. Hamilton wrote more than 50 newspaper essays to sway his fellow New Yorkers in favor of ratification. James Madison and John Jay also contributed to this series, which is known today as *The Federalist*. It remains the starting point for any serious analysis of the Founding Fathers' intentions. Hamilton devoted eight essays to military affairs, presenting a point-by-point refutation of the main Anti-Federalist objections to a national government with definite military power.<sup>52</sup>

Hamilton had been trying to sell his countrymen on the wisdom of military preparedness since 1783, and that served as his chief justification for the Army Clause. He reasoned that stopping Congress from raising troops until a war actually erupted would leave the republic vulnerable to foreign threats. Hamilton insisted,

The United States would then exhibit the most extraordinary spectacle which the world has yet seen, that of a nation incapacitated by its Constitution to prepare for defense before it was actually invaded. . . . We must receive the blow before we could even prepare to return it. . . . We must expose our property and liberty to the mercy of foreign invaders and invite them by our weakness to seize the naked and defenseless prey, because we are afraid that rulers, created by our choice, dependent on our will, might endanger that liberty by an abuse of the means necessary to its preservation.

Even though America's location made a trans-Atlantic invasion improbable, Congress had to be able to reinforce frontier garrisons to keep the Indians in check and deter British and Spanish incursions into the western territories. Hamilton also held "that seditions and insurrections are, unhappily, maladies as inseparable from the body politic as tumors and eruptions from the natural body." That sad reality caused him to conclude: "Should such emergencies at any time happen under the national government, there could be no remedy but force."<sup>53</sup>

Hamilton underscored his preparedness argument with a rationale for military professionalism that would pass muster today: "War, like most other things, is a science to be acquired and perfected by diligence, by perseverance, by time and by practice." Since such a level of commitment could not be expected of the militia, it was imperative that the United States possess a regular force. Hamilton must have struck an even more responsive chord by reminding his readers "how little the rights of a feeble government are likely to be respected, even by its own constituents."<sup>54</sup>

In spite of all this, Hamilton conceded that America's distance from Europe freed it from the need for a large standing army. He also added that many years would pass before the national government could acquire the financial means required to raise a standing army sufficient in size to enslave the populace. Americans could take further comfort from the fact that the army's size would be decided by Congress, the branch of government least likely to foment military coups, as it "was to be a popular body, consisting of the representatives of the people periodically elected." Finally, Hamilton portrayed the 2-year limit on military appropriations as "a great and real security against military establishments without evident necessity."<sup>55</sup>

Turning to the Militia Clause, Hamilton applauded the prospect of national regulation. He observed,

It requires no skill in the science of war to discern that uniformity in the organization and discipline of the militia would be attended with the most beneficial effects, whenever they were called into service for the public defense.

Stealing the rhetoric of the Anti-Federalists, he insisted that the existence of a "well-regulated militia" would dissuade Congress from expanding the regular army. "If the federal government can command the aid of the militia in those emergencies which call for the military arm in support of the civil magistrate," he theorized, "it can the better dispense with the employment of a different kind of force."

Hamilton ridiculed the slightest suggestion that the national government would ever dare to order the militia to curtail state rights. "Where in the name of common sense," he exclaimed, "are our fears to end if we may not trust our sons, our brothers, our neighbors, our fellow-citizens?" As for anxieties regarding distant militia deployments, he replied:

In times of insurrection, or invasion, it would be natural and proper that the militia of a neighboring State should be marched into another, to resist a common enemy, or to guard the republic against the violence of faction or sedition.<sup>56</sup>

The Constitution's ratification did not automatically open the door to a strong military in America. After studying the ratification process, historian Richard Kohn concluded that the public felt uneasy about the new government's military powers. Kohn reported,

Nearly every state's ratifying convention proposed amendments . . . that either warned against standing armies, limited Congress's power to raise forces, or banned quartering of regulars in private homes. Several conventions suggested restrictions on calling up the militia, marching it out of state, or subjecting militiamen to martial law in peacetime.

The First Congress responded to these reservations by quickly passing the ten constitutional amendments comprising the Bill of Rights. The Second Amendment guaranteed the survival of the militia by forbidding Congress to disarm the people. The Third Amendment banned the quartering of troops in private residences.<sup>57</sup>

Hobbled by public opinion and a growing political opposition that cried foul at any effort to broaden federal power, President George Washington's administration steered a cautious course in military matters. On April 30, 1790, it obtained a modest increase in the regular army's enlisted strength from 840 to 1,216. Yet when Brigadier General Josiah Harmar organized a punitive expedition aimed at the Indians north of the Ohio River later in the

year, only 353 regulars could be spared from their scattered posts for field service. Harmar reverted to past practice by augmenting his column with 1,133 militiamen. In two encounters with the Indians, the militia bolted at the first flurry of shots, leaving 75 regulars to be slaughtered.<sup>58</sup>

Harmar's failure to pacify the Indians prompted the Washington Administration to ask Congress for more regulars, but only enough to give the army a second infantry regiment. With the militia discredited and the public still skittish about standing armies, the administration pinned its hopes on a new class of citizen-soldiers, the "Corps of Levies." Recruited for 6 months and subjected to regular army discipline, the 2,000 "levies" were supposed to be more steadfast than militia, but cheaper and more politically acceptable than regulars. Unfortunately, recruiting for both levies and regulars proceeded slowly, and Major General Arthur St. Clair had to call out 418 unruly Kentucky militia to raise his field forces to 2,400 men. Early on November 3, 1791, about 1,000 Indian braves surprised St. Clair and 1,400 partially trained troops in an unfortified camp 100 miles north of Cincinnati. St. Clair and half of his men managed to claw their way clear of a closing ring of death, but 657 soldiers perished in the costliest Indian defeat ever suffered by the U.S. Army.<sup>59</sup>

Driven to desperation by the St. Clair disaster, President Washington urged Congress to approve a 5,000-man regular army. Congress complied on March 5, 1792. Washington and Secretary of War Henry Knox organized this new force into four self-contained mini-armies known collectively as the "Legion of the United States." Major General Anthony Wayne devoted 2 years of drill, discipline, and flogging to mold the Legion into a superb offensive tool, finally leading it to victory at Fallen Timbers on August 20, 1794.<sup>60</sup>

Although the Washington Administration provided America with a small but respectable standing army, it fell short of achieving meaningful militia reform. In January

1790, Secretary Knox submitted his "Plan for the General Arrangement of the Militia of the United States" to Congress. Knox assumed that "an energetic National Militia is to be regarded as the CAPITAL SECURITY of a free republic," which meant that the country could thrive without a lot of regulars. To realize this vision, he advocated more military training and education for the citizenry, as well as classing the militia by age. The "Advanced Corps" would contain men between the ages of 18 and 20, the "Main Corps" 21- to 45-year-olds, and the "Reserved Corps" all remaining militia up to age 60. Knox conceived of the Advanced Corps as "a school in which the youth . . . are to be instructed in the art of war" in annual "CAMPS OF DISCIPLINE." It would also comprise a ready reserve of 32,500 men.<sup>61</sup>

Knox's plan proposed placing the militia under effective national control, and that alarmed both state authorities and the public. Hence, Congress ignored the issue of militia reform until the St. Clair disaster forced its hand. When Congress passed the Uniform Militia Act on May 2, 1792, it empowered the President to call out the militia to execute the laws of the United States against "combinations too powerful to be suppressed by the ordinary course of judicial proceedings." At the same time, Congress stipulated that no militiaman would have "to serve more than 3 months in any 1 year." The legislation also mentioned no mechanism to compel state compliance with federal standards in training, organization, or weaponry.<sup>62</sup>

Despite these weaknesses, President Washington invoked the Uniform Militia Act 2 years later to send 15,000 federalized citizen-soldiers into western Pennsylvania to quell the so-called "Whiskey Rebellion." Some historians question whether there was an uprising at all, charging the Washington Administration with overreacting to a few violent incidents and protest meetings. The excise tax on whiskey, which Congress instituted in March 1791 to help pay down the national debt, provoked immediate resistance, but trouble was not confined to Pennsylvania. It

flared up in Kentucky, as well as parts of Virginia, North Carolina, and South Carolina. Nevertheless, Pennsylvania tax resisters went to lengths that particularly irritated the Washington Administration, tarring and feathering one tax collector and another federal agent.<sup>63</sup>

The situation took on the guise of a major crisis in the summer of 1794 after tax opponents attacked the Allegheny County estate of John Neville, the excise inspector for western Pennsylvania. Twelve regulars from nearby Fort Pitt were detailed to guard Neville's property, but they were overwhelmed by 500 rioters on July 17. As far as Washington was concerned, such blatant defiance of federal authority could not be ignored. He announced that Neville's assailants "have at length been hardy enough to perpetrate acts which . . . amount to treason, being overt acts of levying war against the United States."<sup>64</sup>

When Pennsylvania authorities hesitated to move against the insurrectionists, Washington decided on direct federal intervention. Alexander Hamilton, Washington's Secretary of the Treasury and the father of the excise tax, was the cabinet's most ardent advocate of a military response. He urged the President to mount an awe-inspiring demonstration of national power. Hamilton wrote,

The force ought if attainable to be an imposing one, such if practicable, as will deter from opposition, save the effusion of the blood of Citizens and secure the object to be accomplished.<sup>65</sup>

Washington heeded Hamilton's counsel. The President's approach could best be described as the moderate use of irresistible force. With the regular army committed to the Fallen Timbers Campaign, Washington had no choice but to rely on the militia. He called out a total of 15,000 men from Pennsylvania, New Jersey, Maryland, and Virginia—a larger array than the field army that followed him throughout most of the Revolution. Yet even as the President conjured this massive show of strength, he took

pains to ameliorate the sting of coercion with the balm of restraint. He publicly admitted to “feeling the deepest regret” for having to adopt a force policy.<sup>66</sup> He also reminded Governor Henry Lee of Virginia, who led the federalized militia into the disaffected counties, that the troops’ mission was to restore civil authority and not institute martial law:

Every officer and soldier will constantly bear in mind that he comes to support the laws and that it would be peculiarly unbecoming in him to be in any way the infractor of them; that the essential principles of free government confine the provinces of the Military to these two objects: 1st: to combat and subdue all who may be found in arms in opposition to the National will and authority; 2dly to aid and support the civil Magistrate in bringing offenders to justice. The disposition of this justice belongs to the civil Magistrate and let it ever be our pride and glory to leave the sacred deposit there unviolated.<sup>67</sup>

The whiskey rebels fled at the approach of Lee’s host. This turn of events prompted Washington to exult:

The western insurrection has terminated [in a way] highly honorable for this country; wch. By the energy of its Laws and the good disposition of its citizens have brought the rioters to a perfect sense of their misconduct without spilling a drop of blood.<sup>68</sup>

Washington also depicted the outcome of the Whiskey Rebellion as proof that the Constitution had equipped Americans with the means to maintain domestic tranquility:

It has demonstrated, that our prosperity rests on solid foundations; by furnishing an additional proof, that my fellow citizens understand the true principles of government and liberty; that they feel their inseparable union: that . . . they are now as ready to maintain the authority of the laws against licentious invasions, as they were to defend their rights against usurpation. It has been a spectacle, displaying to the highest advantage, the value of Republican Government, to behold the most and least wealthy of our citizens standing in

the same ranks as private soldiers; pre-eminently distinguished by being the army of the constitution.<sup>69</sup>

Victory did not make Washington arrogant, and he wisely chose to temper justice with mercy. Federal authorities tried 20 insurrectionists for high treason and convicted two. Before they could be executed, however, the President pardoned them. He explained his conduct in his annual address to Congress:

For though I shall always think it a sacred duty, to exercise with firmness and energy, the Constitutional powers with which I am vested, yet it appears to me no less consistent with the public good, than it is with my personal feelings, to mingle in the operations of government, every degree of moderation and tenderness, which the national justice, dignity and safety permit.<sup>70</sup>

When all was said and done, Washington grasped one salient point—that republican government ultimately rests on the love and support of the people. It should not unleash the military against a disaffected minority simply to preserve its own dignity, but to enforce the will of the majority as embodied in laws approved by the people's elected representatives. This lesson was lost on Alexander Hamilton and some of his friends. They came out of the Whiskey Rebellion believing that force was the main prop of stable government. Later during the presidency of John Adams, these "High Federalists" would attempt to deter rebellion by burdening America with a large standing army. This shift toward militarism played into the hands of Thomas Jefferson and the Republican opposition. The Republicans painted the Federalists as the champions of military despotism and the armed forces as a partisan tool. The resulting popular outrage brought an end to Federalist control of the national government in the election of 1800. This transfer of power also ushered in a period of austerity for the military establishment.<sup>71</sup>

The election of 1800 closed a crucial chapter in the evolution of American military policy. It stands as an object



lesson in the risks run by American politicians who abandon moderation and seem too prone to apply force against their fellow citizens. Americans want to feel safe, but they do not want a government that fears them and sees threats where none exist. What Washington termed the “army of the constitution” gambles with its credibility and its future whenever it is made to look like a deterrent to peaceful dissent or a loyal opposition. In our own era, with its conspiracy theories and widespread mistrust of big government, many Americans, like their forebears, are too easily inclined to view the armed upholders of federal authority as the primary threat to the homeland.<sup>72</sup>

## CHAPTER 2 - ENDNOTES

1. On September 29, 1789, Congress mandated the first loyalty oath for the U.S. Army under the Constitution:

That all commissioned and non-commissioned officers, and privates, who are, or shall be, in the service of the United States, shall take the following oaths or affirmations, to wit: “I, A.B., do solemnly swear or affirm (as the case may be) that I will support the constitution of the United States.” “I, A.B., do solemnly swear or affirm (as the case may be) to bear true allegiance to the United States of America, and to serve them honestly and faithfully, against all their enemies or opposers whatsoever, and to observe the orders of the President of the United States of America, and the orders of the officers appointed over me.”

“An Act to Recognize and Adapt to the Constitution of the United States, the Establishment of the Troops Raised under the Resolves of the United States Congress Assembled and for Other Purposes, September 29, 1789,” in Robert K. Wright, Jr., and Morris J. MacGregor, Jr., eds., *Soldier-Statesmen of the Constitution*, Washington, DC: Center of Military History, United States Army, 1987, pp. 57, 234.

2. “Constitution of the United States, September 17, 1787,” in Wright and MacGregor, p. 214.

3. Richard H. Kohn, *Eagle and Sword: The Federalists and the Creation of the Military Establishment in America, 1783-1802*, New York: Free Press, 1975, pp. xii-xiii, 277-93.

4. For an entertaining interpretation of the role war has played in shaping the American character, see Geoffrey Perret, *A Country Made by War: From the Revolution to Vietnam, the Story of America's Rise to Power*, New York: Random House, 1989; Kohn, *Eagle and Sword*, pp. 2-3, 6, 73, 75-76, 109-10, 183-86.

5. Gregory J. W. Urwin, *The United States Infantry: An Illustrated History, 1775-1918*, New York: Sterling Publishing Co., Inc., 1991, pp. 9-10.

6. Kohn, *Eagle and Sword*, p. 7; Allan R. Millett and Peter Maslowski, *For the Common Defense: A Military History of the United States of America*, New York: Free Press, 1994, pp. 2-4.

7. James Kirby Martin and Mark Edward Lender, *A Respectable Army: The Military Origins of the Republic, 1763-1789*, Arlington Heights, IL: Harlan Davidson, Inc., 1982, pp. 16-17; Wright and MacGregor, pp. 5-6; Kohn, *Eagle and Sword*, p. 7.

8. Wright and MacGregor, p. 6; Martin and Lender, pp. 17-18; Kohn, *Eagle and Sword*, pp. 7-8; Urwin, pp. 11-12. Fred Anderson takes a contrary position on the composition of Provincial units. In an impressively researched study, he argues that the regiments Massachusetts fielded for the French and Indian War were truly representative of Bay Colony society:

The army was not heavily weighted with vagrant and marginal elements; while such men clearly made up a segment of the organization, they composed only a small minority of its membership, probably not much greater than their share of the population at large.

Fred Anderson, *A People's Army: Massachusetts Soldiers and Society in the Seven Years' War*, New York: W. W. Norton & Company, 1985, p. 55.

9. Kohn, *Eagle and Sword*, pp. 2, 3; Martin and Lender, pp. 6-15.

10. "Essays by the Impartial Examiner, *Virginia Independent Chronicle*, February-June 1788," in Herbert J. Storing, ed., *The Complete Anti-Federalist*, 7 vols., Chicago: University of Chicago Press, 1981, Vol. 5, p. 181. For more documents that echo these sentiments, see Richard H. Kohn, ed., *Anglo-American Antimilitary Tracts, 1697-1830*, New York: Arno Press, 1979.

11. Kohn, *Eagle and Sword*, pp. 5-6; Wright and MacGregor, p. 11; Martin and Lender, pp. 20-28. For a detailed examination of these issues, see John Shy, *Toward Lexington: The Role of the British Army in the Coming of the American Revolution*, Princeton: Princeton University Press, 1965.

12. Martin and Lender, pp. 1-3, 35-36, 40; Robert K. Wright, Jr., *The Continental Army*, Washington, DC: Center of Military History, United States Army, 1983, pp. 20-25.

13. Martin and Lender, pp. 69-78, 87-97, 131-33; Urwin, *United States Infantry*, pp. 22-25.

14. Kohn, *Eagle and Sword*, pp. 9-13.

15. Wright and MacGregor, *Soldier-Statesmen*, pp. 14, 23; John Shy, *A People Numerous and Armed: Reflections on the Military Struggle for American Independence*, New York: Oxford University Press, 1976, pp. 165-79, 193-24.

16. Merrill Jensen, *The Founding of a Nation: A History of the American Revolution, 1763-1776*, New York: Oxford University Press, 1968, pp. 602-31. See also Jack N. Rakove, *The Beginnings of National Politics: An Interpretive History of the Continental Congress*, New York: Alfred A. Knopf, 1979.

17. In the formative years of the Union, some political theorists argued that the inclusion of the words "common defence" and "general Welfare" in the Constitution endowed Congress with unlimited power to ensure national security. An aged James Madison disagreed with that interpretation. He insisted that those phrases were copied from the Articles of Confederation with little thought or discussion. They simply denoted the Founding Fathers' intent that the new government assume responsibility for the public debt incurred during the War for Independence and under the remaining life of the Confederation. John Dickinson, "John Dickinson's Draft of the Articles of Confederation," in Wright and MacGregor, pp. 183-85; James Madison to Andrew Stevenson, November 17, 1830, in Max Farrand, ed., *The Records of the Federal Convention of 1787*, 4 vols., New Haven: Yale University Press, 1966, Vol. 3, pp. 484-88.

18. "The Articles of Confederation, March 1, 1781," in Wright and MacGregor, pp. 187-188.

19. An authoritative examination of the impact of the Confederation's weaknesses on the Continental Army is E. Wayne

Carp, *To Starve the Army, at Pleasure: Continental Army Administration and American Political Culture, 1775-1783*, Chapel Hill: University of North Carolina Press, 1984.

20. According to Richard H. Kohn, the "Newburgh Conspiracy" was encouraged in part by Governor Morris, Alexander Hamilton, and other nationalists in Congress as a ploy to intimidate the states into sharing the power to tax with the Confederation government. Kohn, *Eagle and Sword*, pp. 17, 23, 25-27, 31-36, 38; Martin and Lender, pp. 160-65, 186-95; Wright, *Continental Army*, pp. 177-182; Urwin, *United States Infantry*, p. 29.

21. Kohn, *Eagle and Sword*, p. 42.

22. Before Washington responded to Hamilton's committee, he solicited the views of some of his senior officers. Friedrich von Steuben, the Continental Army's inspector general, advocated a peace establishment of 4,000 regulars, including a 120-man "Corps of Horse." The latter would "be employed in guarding the residence of Congress, the public offices, papers, etc." As Steuben elaborated: "Congress and their executive officers should never be exposed to the mad proceedings of a mob. Guards are necessary and proper at the seat of government." The Prussian drillmaster also called for a select, well-disciplined militia of 21,000 "ready to act on the shortest notice." George Washington, "Sentiments on a Peace Establishment, May 2, 1783"; Friedrich von Steuben, "A Letter on the Subject of an Established Militia, and Military Arrangements, Addressed to the Inhabitants of the United States, 1784," both in Wright and MacGregor, pp., 193-200, 202-7; Kohn, *Eagle and Sword*, pp. 42-47.

23. Kohn, *Eagle and Sword*, pp. 47-53; Wright, *Continental Army*, pp. 181-182; Urwin, *United States Infantry*, pp. 29-30.

24. Wright and MacGregor, p. 29; Kohn, *Eagle and Sword*, p. 60; Urwin, *United States Infantry*, pp. 30-32.

25. Urwin, *United States Infantry*, pp. 30-32; For more details on the short, inglorious history of the 1st American Regiment, see James Ripley Jacobs, *The Beginning of the U.S. Army 1783-1812*, Princeton: Princeton University Press, 1947; and William H. Guthman, *March to Massacre: A History of the First Seven Years of the United States Army, 1784-1791*, New York: McGraw-Hill Book Company, 1975.

26. Kohn, *Eagle and Sword*, pp. 74; Wright and MacGregor, pp. 32-33. For differing interpretations on the role of mob violence in the revolutionary movement, see Hiller B. Zobel, *The Boston Massacre*, New

York: W. W. Norton & Company, Inc., 1970; Edmund S. Morgan and Helen M. Morgan, *The Stamp Act Crisis: Prologue to Revolution*, New York: Collier Books, 1963; Pauline Maier, *From Resistance to Revolution: Colonial Radicals and the Development of American Opposition to Britain, 1765-1776*, New York: W. W. Norton & Company, 1992; Gordon S. Wood, *The Radicalism of the American Revolution*, New York: Random House, 1993; Gary B. Nash, *The Urban Crucible: The Northern Seaports and the Origins of the American Revolution*, Cambridge: Harvard University Press, 1986.

27. Wright and MacGregor, p. 33; Kohn, *Eagle and Sword*, pp. 74-75; George Washington to Henry Knox, December 26, 1786, in W. W. Abbott and Dorothy Twohig, eds., *The Papers of George Washington: Confederation Series*, 6 vols., Charlottesville: University Press of Virginia, 1992-97, Vol. 4, pp. 481-482.

28. George Washington to David Humphreys, December 26, 1786, in Abbott and Twohig, Vol. 4, p. 478.

29. George Washington to Marquis de Lafayette, March 25, 1787; George Washington to Marquis de Lafayette, August 15, 1787, both in Abbott and Twohig, Vol. 5, pp. 106, 296; Wright and MacGregor, pp. 33-34.

30. Wright and MacGregor, pp. 33-34, 45; Kohn, *Eagle and Sword*, pp. 73, 75; Farrand, Vol. 1, pp. 19.

31. Farrand, Vol. 1, pp. 20, 30.

32. Kohn, *Eagle and Sword*, pp. 75-76; Wright and MacGregor, p. 40; George Washington to Marquis de Lafayette, August 15, 1787, in Abbott and Twohig, Vol. 5, p. 296; Farrand, Vol. 1, pp. 246, 285.

33. Mason's words, as quoted here, come from the notes kept by Rufus King of Massachusetts. James Madison, another member of the Virginia delegation, recalled Mason as saying:

What, would you use military force to compel the observance of a social compact? It is destructive to the rights of the people. Do you expect the militia will do it, or do you mean a standing army? The first will never, on such an occasion, exert any power; and the latter may turn its arms against the government which employs them.

Mason and Madison both accepted an American standing army as a necessary evil, but they wanted the Constitution to acknowledge that

"standing armies in time of peace" posed a threat to "the liberties of the people." This motion was rejected at the urging of New York's Governor Morris, who pointed out that such a caveat would place "a dishonorable mark of distinction on the military class of Citizens." Kohn, *Eagle and Sword*, pp. 77-78, 80, 87-88; Farrand, Vol. 1, pp. 246, 332, 346, 349, and Vol. 2, p. 617; Wright and MacGregor, pp. 40.

34. "Constitution of the United States, September 17, 1787," in Wright and MacGregor, pp. 216.

35. *Ibid.*, p. 217.

36. As a member of the Confederation Congress in 1783, Gerry helped lead the fight against a peacetime military establishment. Kohn, *Eagle and Sword*, pp. 52-53; Farrand, Vol. 2, pp. 317, 329.

37. Farrand, Vol. 2, pp. 326, 330, 384-385.

38. *Ibid.*, Vol. 2, p. 385.

39. "Constitution," in Wright and MacGregor, pp. 215-17; Farrand, Vol. 2, pp. 317, 330, 386-388, 422, 426-427, 505-506, 509.

40. Wright and MacGregor, pp. v, 3, 42; Kohn, *Eagle and Sword*, pp. 81.

41. Kohn, *Eagle and Sword*, pp. 82. For a sampling of typical Anti-Federalist denunciations of standing armies, see "A Review of the Constitution Proposed by the Late Convention by A Federal Republican, 1787," in Storing, Vol. 3, p. 76; "A Letter from a Gentleman in a Neighboring State, to a Gentleman in this City, *Connecticut Journal*, October 17 and 24, 1787"; "Essay by Samuel, (*Boston*) *Independent Chronicle and Universal Advertiser*, January 10, 1788"; "Observations On the New Constitution, And on the Federal and State Conventions By A Columbian Patriot, Boston, 1788," all in Storing, Vol. 4, pp. 12, 193, 277; "Essays by A Farmer, (*Baltimore*) *Maryland Gazette*, February-April 1788"; "Letter of Richard Henry Lee to Governor Edmund Randolph, October 16, 1787"; "Essays by The Impartial Examiner," *Virginia Independent Chronicle*, February-June 1788," all in Storing, Vol. 5, pp. 22, 27-28, 116, 181.

42. "Essays by Cincinnatus, *New York Journal*, November-December 1787"; "Objections by A Son of Liberty, *New York Journal*, November 8, 1787," both in Storing, Vol. 6, pp. 17, 34; "Essays of Phladelphiensis, (*Philadelphia*) *Independent Gazetteer*, November 1787-April 1788"; "The Address and Reasons of Dissent of the Minority of the Convention of Pennsylvania to Their Constituents," *Pennsylvania*

*Packet and Daily Advertiser*, December 18, 1787," both in Storing, Vol. 3, pp. 114, 164; "Essays of John De Witt, (*Boston*) *American Herald*, October-December 1787", in Storing, Vol. 4, p. 23.

43. "Letters of Agrippa, *Massachusetts Gazette*, November 1787-February 1788," in *Ibid.*, Vol. 4, p. 78.

44. "Speeches of Patrick Henry in the Virginia State Ratifying Convention," in *Ibid.*, Vol. 5, p. 217.

45. "The Genuine Information, Delivered to the Legislature of the State of Maryland, Relative to the Proceedings of the General Convention, Held at Philadelphia, in 1787, By Luther Martin, Esquire, Attorney-General of Maryland, and One of the Delegates in the Said Convention," *Maryland Gazette and Baltimore Advertiser*, December 28, 1787-February 8, 1788, in Farrand, Vol. 3, p. 218.

46. "A Letter from a Gentleman in a Neighbouring State, to a Gentleman in this City, *Connecticut Journal*, October 17 and 24, 1787," in Storing, Vol. 4, p. 11.

47. "Address of John Humble, (*Philadelphia*) *Independent Gazetteer*, October 29, 1787"; "Philadelphiensis Essays," both in *Ibid.*, Vol. 3, pp. 90, 111, 114.

48. Kohn, *Eagle and Sword*, pp. 83; "Observations By A Columbian Patriot," in Storing, Vol. 4, p. 277; "Impartial Examiner Essays"; "Address by Denatus, *Virginia Independent Chronicle*, June 11, 1788," both in Storing, Vol. 5, pp. 182, 265-266.

49. "Essay of A Democratic Federalist, *Pennsylvania Herald*, October 17, 1787," in Storing, Vol. 3, p. 62.

50. James Monroe, "Some Observations on the Constitution, 1788," in *Ibid.*, Vol. 5, p. 292.

51. "Luther Martin before the Maryland House of Representatives," November 29, 1787, in Farrand, Vol. 3, p. 157; "Letter from a Gentleman," in Storing, Vol. 4, p. 12; "Son of Liberty," in Storing, Vol. 6, p. 35.

52. Hamilton wrote 51 of the essays comprising *The Federalist*, while Madison wrote 26 and John Jay, 5. In addition, Hamilton and Madison co-authored three more, making a total of 85. Clinton Rossiter, "Introduction," in Alexander Hamilton, James Madison, and John Jay, *The Federalist Papers*, New York: New American Library, 1961, pp. x-xi.

53. Kohn, *Eagle and Sword*, pp. 84; Hamilton, Madison, and Jay, pp. 160-163, 165-166, 168, 178.

54. Hamilton, Madison, and Jay, pp. 161, 166-167.

55. *Ibid.*, 69, 71, 158, 171-172, 182.

56. *Ibid.*, 173-174, 182-184, 186-187.

57. Kohn, *Eagle and Sword*, pp. 85-86; Wright and MacGregor, pp. 45.

58. Kohn, *Eagle and Sword*, pp. 92, 96, 102-103, 106, 108, 174-175; Guthman, pp. 173-197; Urwin, p. 32.

59. The Corps of Levies may have proven unequal to the exigencies of Indian-fighting, but as Richard Kohn explained, it left an important legacy to the American military tradition:

Levies were the embryo of the federal volunteer system which was destined to become the backbone of America's wartime armies in the nineteenth century, and with selective service, the basis for the mass armies in the age of total war and cold war.

Kohn, *Eagle and Sword*, pp. 109-110, 114; Guthman, pp. 206-244; Urwin, pp. 32-33.

60. Urwin, pp. 33-37; Kohn, *Eagle and Sword*, pp. 120, 122-123, 125-126.

61. Henry Knox, "Plan for the General Arrangement of the Militia of the United States, January 18, 1790," in Wright and MacGregor, pp. 234-241.

62. Kohn, *Eagle and Sword*, pp. 129-35; "An Act More Effectually to Provide for the National Defense, by Establishing an Uniform Militia throughout the United States," in Wright and MacGregor, pp. 244-245.

63. James Kirby Martin, "Introduction: The Whiskey Rebellion Redivivus"; Thomas P. Slaughter, "The Friends of Liberty, the Friends of Order, and the Whiskey Rebellion: A Historiographical Essay"; Mary K. Bonsteel Tachau, "A New Look at the Whiskey Rebellion," all in Steven R. Boyd, ed., *The Whiskey Rebellion: Past and Present Perspectives*, Westport, Connecticut: Greenwood Press, 1985, pp. 3-7, 9-30, 97-100; Kohn, *Eagle and Sword*, pp. 139-40. See also Thomas P. Slaughter, *The Whiskey Rebellion: Frontier Epilogue to the American*



*Revolution*, New York: Oxford University Press, 1986. A reliable summary of George Washington's response to the Whiskey Rebellion may be found in James Thomas Flexner, *Washington: The Indispensable Man*, Boston: Little, Brown and Company, 1974.

64. John Neville to Tench Coxe, July 18, 1794; "Deposition of Francis Mentges," August 1, 1794; Alexander Hamilton to George Washington, August 5, 1794, all in Harold C. Syrett, ed., *The Papers of Alexander Hamilton*, 27 vols., New York: Columbia University Press, 1961-87, Vol. 17, pp. 2-6, 24-58; Kohn, *Eagle and Sword*, p. 161; George Washington, "Proclamation," August 7, 1794, in John C. Fitzpatrick, ed., *The Writings of George Washington*, 39 vols., Washington, DC: U.S. Government Printing Office, 1931-44, Vol. 33, p. 458.

65. "Conference Concerning the Insurrection in Western Pennsylvania," August 2, 1794; Alexander Hamilton to George Washington, August 2, 1794, both in Syrett, Vol. 17, pp. 9-14, 15-19; Kohn, *Eagle and Sword*, pp. 162, 164.

66. Wright and MacGregor, p. 52; Washington, "Proclamation," August 7, 1794, in Fitzpatrick, Vol. 33, p. 460; Edmund Randolph to Thomas Mifflin, August 7, 1794, in Syrett, Vol. 17, p. 71.

67. George Washington to Henry Lee, October 20, 1794; see also George Washington to Daniel Morgan, March 27, 1795, both in Fitzpatrick, Vol. 34, pp. 6, 159-160. For more on Lee's involvement in the Whiskey Rebellion and the politics of the early republic, see Charles Royster, *Light-Horse Harry Lee and the Legacy of the American Revolution*, New York: Alfred A. Knopf, 1981.

68. Kohn, *Eagle and Sword*, pp. 170; George Washington to John Jay, December 18, 1794, in Fitzpatrick, Vol. 34, p. 62.

69. George Washington, "Sixth Annual Address to Congress," November 19, 1794, in Fitzpatrick, Vol. 34, p. 34.

70. George Washington, "Seventh Annual Address to Congress," December 8, 1795, in Fitzpatrick, Vol. 3, p. 390. Major General Benjamin Lincoln reached the same conclusion after leading the Massachusetts militia in quelling Shays' Rebellion. On February 22, 1787, Lincoln confided to his friend, George Washington:

In her right hand Government must hold out such terms of mercy in the hour of success, with such evident marks of a disposition to forgive as shall apply to the feelings of the delinquents, beget in them such sentiments of gratitude and

love by which they will be led to embrace with the highest cordiality that Government which they have attempted to trample under foot.

Benjamin Lincoln to George Washington, December 4, 1786-March 4, 1787, in Abbott and Twohig, Vol. 4, p. 431.

71. Kohn, *Eagle and Sword*, pp. 171-72, 219-68; Edmund Randolph to Thomas Mifflin, August 7, 1794; Alexander Hamilton, "Tully No. III," *American Daily Advertiser*, August 28, 1794; Alexander Hamilton, "Tully No. IV," *American Daily Advertiser*, September 2, 1794, all in Syrett, Vol. 17, pp. 69, 71, 160, 178-179.

72. As Benjamin Lincoln advised George Washington 7 years before the Whiskey Rebellion:

Love and Fear are the bonds of civil Society. Love is the noblest incentive to obedience; a Government supported hereon is certainly the most desirable, and ensures the first degrees of happiness which can be derived from civil compact. Such a Government as this is always wounded, when any thing shall exist which makes it necessary to apply to the fears of the governed. This never will be done by a wise administration, unless the General Good renders it indispensable, and it will be removed the first moment it can be, consistently with the common safety.

Benjamin Lincoln to George Washington, December 4, 1786-March 4, 1787, in Abbott and Twohig, Vol. 4, p. 431. For further reading on the military's place in American life, see Richard H. Kohn, ed., *The United States Military under the Constitution of the United States, 1789-1989*, New York: New York University Press, 1991; and Louis Smith, *American Democracy and Military Power: A Study of Civil Control of the Military Power in the United States*, Chicago: University of Chicago Press, 1951.

## CHAPTER 3

### THE PUBLIC'S EXPECTATIONS OF NATIONAL SECURITY

Peter D. Feaver

When Dr. Tilford asked me to come here, he asked me to look through the data that Richard Kohn and I had collected for the Triangle Institute for Security Studies (TISS) Project on the Gap between the Military and Civilian Society and some other recent polls, and asked me to report on public expectations of security. This is not a comprehensive analysis of public attitudes on defense, but rather touches on several areas of special concern for the issue identified in this year's Army War College Strategy Conference. I have arranged my talk in terms of six provocations. I call them provocations because these are things that I know to be true, but to stimulate debate I am framing them in a more extreme way than I would if I were sitting in a position of responsibility.

First, the public places a higher priority on "on our soil" threats than do elites, both civilian elites and the up-and-coming military officers we surveyed—military officers like those attending this conference today. By the way, in our study we refer to this group of military officers as the "military elite," an admittedly awkward term with unfortunate connotations that we do not necessarily mean. We simply refer to the most promising officers at various stages of their career identified by their attendance in residence at the various professional military education (PME) institutions: staff colleges, war colleges, and the CAPSTONE baby general course.

Second, there is a potential for the presidential campaign context to give these issues a higher salience. Although so far this has not been realized, I see it as a possibility.

Third, public confidence in the military is high, but it is brittle, and there is a potential for the homeland security mission to wreck that confidence.

Fourth, while we are focusing on “on our soil” events, we should not forget that there will be many operations beyond our soil. Indeed, in our study, we have discovered a link between the vanishing veterans phenomenon in our policymaking community and the actual conduct of foreign policy.

Fifth, the policymakers—and also military leaders, but especially policymakers—have bought into a myth that the public is casualty-averse.

And finally, I want to make the point that the CNN effect is real, but it doesn't work like one might think it works. The people who are moved into or out of action by CNN's coverage are not the American public, but the decision-makers.

#### Public Priorities.

The public sees a greater threat and a greater role for the military, but not necessarily because they think the military is more effective than nonmilitary tools. This is an area where Charles Dunlap's surmise in his “Origins of the Coup of 2012” article comes into play; that the public might think that the military tools are more effective than nonmilitary tools. In fact, what we found is that civilians do not think military tools are necessarily more effective than nonmilitary tools: they just think that if the problem is important, we must throw something at it, so we might as well throw the best-equipped, best-funded tool at our disposal—the military. Civilians think the “on our soil” problem is a more serious threat than do the military, and this translates into a greater role for the military than the military would see for itself. The gap is not dramatic—between five and fifteen points, depending on the question—but it is discernible. It underscores my basic

point about public opinion, which is that we do not need to mount an effort to mobilize the public to worry about this threat. It already does, and it thinks that this threat is even graver than military elites believe.

Indeed, the public supports a get tough policy, a retaliation policy, even though it believes that such a retaliation would trigger a counter-retaliation. So with the polling that was done right after the bombings of the embassies in Africa, which led to the cruise missile strikes against the Sudanese pharmaceutical factory and the Afghani terrorist sites, the pollsters asked the public, "Do you support those air strikes against those terrorist installations?" The public said, "Yes," and then were asked, "Do you think that the terrorists will counter-respond?" The public said, "Yes, even more so." Eighty-five percent said they thought that hitting the terrorists would mean the terrorists would hit back and yet they still supported a get tough policy. This suggests that the public is not naïve; it does not believe that taking a single swat at the problem will make it go away, but they still want to take that swat. The public thinks that anti-terrorism laws are too weak; they do not think that the anti-terrorism laws are too strong. Now, there is an influential wing of public opinion that is worried about civil liberties. But the reservoir of the American public is all too willing to toughen anti-terrorism laws even if it is going to shrink civil liberties a little bit—at least that is what they say in public opinion polls. Of course, when their civil liberties are actually infringed upon, that might change.

### Threat Perception.

Now let us take a look at threat perception. These are small gaps, but I would say that the military is not worried about large numbers of refugees pouring across the borders; only 8 percent say that it is a very serious threat. But fully a third of the general public says that it is a very serious threat—a remarkably high number. A similar pattern

appears with terrorist attacks. The military is worried about that, but the general public is worried about it even more so. Interestingly, the one area where the military might be a little bit out in front of civilian opinion is on the issue of cyber threat. It is not clear what this means for our study, if anything.

How important is the military role in this? In each case, the civilian elites gave a slightly greater weight to the military role. They were more inclined to say that this is a very important role for the military. This is consistent with something that Charles Dunlap and others have argued: that this is not the military desperately seeking a role in the post-Cold War era. Rather this is certainly a civilian push in the direction of getting the military involved in these types of issues. This point bears emphasis, since among my academic friends there is a popular canard that DoD is desperately seeking a mission in order to prop up budgets, and one of the types of mission that they stumbled upon is "on our soil" missions. That is not consistent with what is happening in Washington, DC, but it also does not reflect the reading of public opinion, which shows the civilians worrying about this as much, if not more than, the military, and shows the civilians leaning further forward in the saddle to push the military in this direction. The bottom line is that you don't need to mobilize the public to worry about this.

Because of the public's greater concern for "on our soil" threats, and because we are in a Presidential campaign, there is a potential for these issues to have traction in the campaign. Conventional wisdom is that foreign policy is not important: it is a secondary issue. If you go on the websites of the two principal candidates, you have to search long and hard to find important statements on foreign policy. Interestingly enough, Governor Bush's website has much more richness and depth on foreign policy than does Vice President Gore's, but education accounts for about 90 percent of the issue papers on each of their websites. That is consistent with what the candidates are getting from the

public opinion polls. Education is issue number one for the voters, and foreign policy is back around issue number ten. That is the conventional wisdom, but Robert Kagan, senior associate at the Carnegie Endowment for International Peace, myself, and others think that there might be an opportunity for foreign policy to have a play in the campaign.

First, a significant portion of the public says that foreign policy is going to be a very important issue. When voters pick presidents, part of what they are picking is a leader, and part of that image of what is leadership plays itself out in how the president conducts him or herself in foreign affairs. There is at least some electoral advantage for the candidate who can position him or herself as being more of a leader than the others, and using foreign policy as a way to gain some momentum on the leadership issue. This is especially so if the differences on the substance of the major issues, such as education, are not too stark. It is also important to note that, in some polls, as much as 79 percent of the public lists fighting international terrorism as a very important goal. It is ranked fourth, however, because there are many important issues that the voters worry about—but fighting terrorism is still a salient goal for the public. There is a potential for a candidate to tap into that concern. And neither candidate has any real advantages on this issue—this is where I do differ with the conventional, inside-the-beltway, wisdom. Inside the beltway, Governor Bush is viewed as quite vulnerable on foreign policy. After all, he flunked a quiz. (By the way, I think half of my International Relations faculty colleagues and all my other political science colleagues would have flunked that particular quiz.) The conventional view is that Vice President Gore has got foreign policy locked up. But the voters do not think so. If you ask the American people, you will see that they are split right now. To be sure, we have not had many presidential debates yet on foreign policy. Those numbers could shift, and they are tracking poll numbers that literally change every week. They are very volatile, and

the point is there is a potential for either candidate to score on foreign policy.

If one were advising the campaign, what would be some ways to gain traction on “on our soil” issues? One of them is National Missile Defense. In the last 2 years, the administration has gone a long way to removing their vulnerability on this issue. But if you look at the first 6 years of the Clinton administration, it clearly was dragging its feet on National Missile Defense. Whether or not it works—and experts can disagree on what was the appropriate policy—from a public opinion point of view, even from a demagoguery point of view, it is much easier to demagogue and say we should have done more, faster. We put American lives at risk in order to preserve this thing called the Anti-Ballistic Missile (ABM) Treaty. How many Americans are willing to sacrifice Chicago for the ABM Treaty? Very, very few. On that issue, I think the Republicans may have an easier time scoring points than the Democrats.

The second point is, of course, that everyone is opposed to terrorism, so you are not going to get any campaign spokesperson out there saying, “I do not think terrorism is important.” You are not going to get anyone to give a talk on, “Have we over-hyped the threat?” We may have very well over-hyped the threat, but you are not going to get a candidate to say that. Everyone is worried about terrorism, everyone is opposed to it. Who is solving it? It strikes me that the campaign that comes out with the most coherent statement, not just a statement opposing terrorism but one indicating some sort of a plan for doing better than what we are doing now, has an advantage, especially if we suffer a terrorist attack in the next 8 months. At that point it will be too late from a political point of view: Governor Bush could not come out the next day with a sort of a jury-rigged plan for counterterrorism because that would look like—as a friend of mine said—“a drive by shooting playing off the tragedy.” In the immediate aftermath of a tragedy such as a terrorist attack on the United States, there will be a rally-around-



the-flag effect. We will see Vice President Gore's poll numbers go up. The Republicans would have no traction at that moment, unless they have already laid out a comprehensive vision on this issue, and this vision is somewhat richer and more robust than the Democrats' vision, in which case in the weeks' aftermath of that event the Republicans would get some campaign traction.

I would mention at this point that it is the considered judgement of our top law enforcement officials and our top national security officials that we were extremely lucky that we did not have one of those in January or February, in the middle of the primary campaign. It was good intelligence and proactive measures but by all accounts there was a large element of luck, which means we could have one of those events in the future. And such an event could be a very crystallizing experience if it happened during the campaign, so there is a potential for this to be a bigger issue. Now, as you heard this morning, the expert consensus is that the government has not solved the puzzle. It is a very difficult problem, but if you are looking for cheap shots to take at the Gore administration, then there are possibilities in this area.

Then, of course, there is the vulnerability on the Sudan factory strike. The American public generally supported that, but the further we move from the time of that strike, the more doubt there is in public opinion. It was clear that there was a breakdown within the administration, at least in the intelligence cycle: the Sudan portion of it was very closely guarded. Decisionmaking was handled by very, very few individuals, and the Administration is consequently vulnerable on that entire issue.

#### Public Confidence in the Military.

Turning now to the issue of public confidence in the military, our finding here is especially provocative or controversial because we all know the famous Gallop Poll finding that the military is the institution in which the

public has the greatest confidence. That is true. It is a very shallow finding because it is only one question, but it is true. It is also robust; it has held up for a number of years and is much higher than it was in the immediate aftermath of the Vietnam War, when on that very same question, the public rated the military very low—not quite as low as they rate lawyers or even academics, but nevertheless they rated it low in the mid-seventies. The fact that they rate the military high now is good news, and it is important. But that confidence number is brittle, and it is an uncertain foundation. If the military is counting on that as a bulwark against any future problems in civil-military relations, any future problems in funding, or other aspects that it would be concerned about, then the military is being naïve.

First of all, even that one question, public support for the military, is inflated by the presence of veterans in the public sample. If you disaggregate on that question between those who served and those who have not served, those who have not served have lower confidence in the military than those who have served. That means, other things being equal, as the veteran population diminishes over time, that confidence number will drop down as well. It is also true that in an age cohort where there is very high support, namely the “Generation Y” 18- to 25-year-olds, there is also very low accession, or very low probability of serving. It is a little bit of that voyeurism of the American culture today that likes to watch football but does not like to play football. It likes to watch the military, but does not like to join the military. And if we look at the constituent elements of support for the military, whether it is “Are you proud of the military?,” or “Do you think we will have the best military 10 years from now?”—all of those other elements that go into support for the military—then support is weaker. So I agree with David King’s analysis. David King, a professor at Harvard, has studied the last 15 years of that particular poll finding. He basically comes down and says this is a poll finding that is asking, “Did the military do a good job the last time it was sent out to fight?” And the answer is, “Yes, it

has," but it is not reinforced by large numbers of people who have a personal connection to the military, who understand and appreciate military culture, and who would support the military even if circumstances conspired against a "good job" the next time out.

This brings us to the question of homeland defense as a mission. Is this a mission that the military can do well? I do not think it is a mission that the U.S. Government can do well. We do not do grand strategy on this, and here I am merely reinforcing what Dr. Hamre said to you this morning. It also raises the goatherder problem, such as the time when Marines were patrolling the Texas border and inadvertently shot the poor goatherder, thinking he was a smuggler. I believe that a homeland defense is rife with those kinds of dangers or pitfalls. Also, there is the basic case of asymmetry of the threat: to do homeland defense, you have to be successful everywhere at all times; to undo American homeland defense, you just have to be successful once. One of our major findings in this entire culture study that we did is that the public does not understand civil-military relations, nor does it really understand the background that you heard earlier. To the extent that homeland defense puts strains on civil-military relations, it just exacerbates it.

### Questions Beyond U.S. Soil.

While we are worrying about homeland defense, I am here to tell you that foreign operations are likely to increase. I suspect this to be true because of several factors, but Christopher Gelpi, a Duke colleague who was part of the TISS study team, and I found one somewhat surprising factor: the propensity to use force is associated with the presence of veterans in the policymaking elite. It turns out that veterans, with some qualifications, think rather along the lines of the Powell Doctrine. On the other hand, civilian elites who have not served in the military think a little bit more like the Madeleine Albright Doctrine approach to the

use of force. If you track the presence of veterans in the policymaking elite in the Cabinet and Congress over time, from 1816 to 1992, you will find a very strong correlation: the more veterans in that policymaking elite, the less likely the United States is to use force. But if the United States does use force and there are a lot of veterans, it will be a much larger effort. This is what we would expect if we extrapolated from the Powell Doctrine to U.S. behavior, controlling for all the other factors that contribute to the use of force.

The percentage of veterans in the political elite is going down, as William Bianco, another TISS study team member, discovered. For 75 years, from 1900 to about 1975, there was always a 10- or 15-point “veterans bonus” in the Congress. And with the end of the draft—but it is not just the draft, because this bonus predated the draft—and with the end of Vietnam and the end of party strength and other factors that have contributed to it, the veterans premium disappeared. This is the future political environment for our policymaking elite. There will be fewer and fewer veterans. If we strap that on to our previous statistical findings, it leads us to the expectation—other things being equal, of course—of ever higher rates of U.S. use of force.

The Public is not Casualty-Adverse.

My fifth point is the one that former U.S. Army War College Commandant Major General Robert H. Scales disagrees with, as he said when he spoke in my venue, so I take particular relish in advancing it here on his turf. Policymakers and the elites think the public is casualty shy, but the public is not. Our survey asked both whether the respondent thought the public was casualty-sensitive and also asked about the respondent’s own sensitivity to casualties. Elites overwhelmingly thought the general public was casualty shy, but the general public respondents, when reporting on their own attitudes toward casualties, did not exhibit much casualty shyness. When we asked

about high intensity missions like Korea or Taiwan, the public answer for how many casualties are acceptable in order to accomplish the mission was remarkably high. Of course, all casualties are "unacceptable" in one sense, but if you have to take casualties to accomplish a mission, the public is as acceptant as our military elites. Then when we asked about nontraditional missions, we got a wide gap, although not in the direction we might have expected. The civilian responses are two to four times higher, more acceptant, than the military responses. It is not the public that is casualty-averse, it is policymakers, perhaps in the White House, but also the military elite.

### The CNN Effect.

Finally, people think that the public is casualty-shy because they think the public responds to the CNN effect. But the CNN effect does not work on the public. First of all, the public is not watching CNN; the policymakers in Washington are. But the people who are moved by CNN are the policymakers themselves. Who whipsawed us into Somalia? It was via CNN, but it was President Bush who was watching CNN. He admitted as much in a speech that he gave in Houston last fall. He said he was watching the coverage of the famine on television and came to the conclusion that the suffering was terrible and so got on the phone to Secretary Cheney to say that something must be done. Who whipsawed us out of Somalia? It was not the general public; their support for the operation was eroding before the disastrous Mogadishu raid and did not drop precipitously until after President Clinton as much as said that this was a war the United States could not win and so the administration was going to pull out. At that point, public support dropped. CNN may whipsaw the policymakers, but it does not do so via CNN's effect on public opinion.

## Conclusion.

In conclusion, I believe these six points to be true. I've exaggerated them for effect, but I would be happy to defend them in questions. I will leave you with the bottom-line bumper sticker of our study: *the quality of civilian leadership matters*. All of these problems can be ameliorated with better civilian leadership. All of these problems are exacerbated with bad civilian leadership.

## CHAPTER 4

### SECURITY EXPECTATIONS FOR TRANSNATIONAL CORPORATIONS

George K. Campbell

My role is to provide a perspective on what keeps many of us in the American business security infrastructure awake at night. These remarks are influenced by an insatiable desire for information in a land where sharing is an often unfruitful, unidirectional activity. Therein lies my message.

In the interests of further establishing bias up front, "us" comprises a body at least four times the size of that devoted to public protection at all levels in the United States. This resource reality is a dynamic that must be considered in the evolving definition of our national security infrastructure. In my humble view, "national security" will increasingly rely upon developing a new order of the business-government relationship to include these private assets as players of critical value in the chain of protection.

As to the theme, I wonder what a contemporary version of the Federalist Papers written by the framers of this new public-private order might say about "insuring domestic tranquility and providing for the common defense" in the new millennium? What are the elements of a "realistic domestic security environment"? What set of likely threats and whose assessment of vulnerability frame the debate? International boundaries melt before the self-interests of interconnected, interdependent global players owing allegiance to private shareholders vs. franchised citizens. Whose reality are we discussing here?

As to Fidelity's business, we are the world's largest privately owned financial services firm with over \$1 trillion in assets under management along with a multiplicity of entrepreneurial businesses stretched across the globe. For

myself, I am expected by my employer to anticipate in pre-real time the global threats confronting Fidelity Investments' 33,000 employees, 17 million customers, global technical backbone, business continuity and market reputation. Like many of you, my work is about aligning our limited resources against higher likelihood threats and ensuring that our response capabilities are adequately positioned and prepared. The mission of my organization is to add value to our business by enabling it to do things that would otherwise be too risky. What keeps my attention is that my list of risks is another's list of opportunities.

What about risk? I believe the most pervasive, highest likelihood threat to the security environment of American business is rooted in our absolute, pervasive and growing reliance on information technology. Our prior experience in the application of proven protection measures around physical assets is now tested against a virtual landscape moving at warp speed around which we must establish a reliable, defensible perimeter. A perimeter through which must pass any number of untrusted enrollees with keys provided by others over whom I have no control. This is the security environment in which we will all live for the foreseeable future. The rules of engagement here are yet to be imagined, let alone written.

At an international security conference we hosted in 1998, Donn Parker of SRI Consulting, tossed out the observation that, until 50 years ago,

humankind has only been able to perform single processes. As computers have become prevalent, humanity has learned to create and own a process and use it repeatedly, not just once. By applying this learning to negative processes—crimes—it is possible for the first time in history to possess and use a crime, not just commit it once. One person can design a crime, another can test and develop it and others can execute copies.

He goes on to define the characteristics of an automated crime.

- It is packaged in a program or suite of programs.



- It performs all parts of the crime, selecting victims, converting to gain, and erasing the evidence.
- It is accomplished instantly, in computer time.
- A perpetrator can execute it without human interaction or without knowledge of the crime.
- Experts can test and repeatedly improve it if it is found to be inadequate.
- It can be designed by one person and executed by others.

Obvious examples of these packaged crimes are found daily in the form of computer viruses and hacker tools. It is coincidental that as I write these remarks, several notable e-businesses are being hit by distributed denial of service attacks. These attacks are absurdly easy to launch and threaten public confidence in the reliability and integrity of these increasingly pervasive business channels. However, far more insidious adversarial capabilities are in the inventory or will be crafted as motive and opportunity combine. For example:

- Look at the direction of information technology and then think about the incredible push to connect the customer to a full service business interaction. The next computer you will buy will fit in your wallet. Welcome to the wireless crypto-dependent, belt-mounted, interactive, very vulnerable, socially engineerable, not really personal business relationship device. How do we really know the virtual customer in a digital relationship and is that a masked man or the legitimate item?
- Fuzzy boundaries defy physical and logical definition. The velocity of E-business masks risk and provides cover for the intruder. How do you define, in very real legal terms, the concepts of access, trust and defensible control in cyber-land? What is a legal standard of "security" in electronic commerce? What planet-wide authority defines and enforces it?

- If I'm attacked, what rights do I have to protect myself in my virtual home? If I counter the attack, may I intrude as I follow the trail of my adversary? What offensive strategy may I pursue as a means of identifying my adversary and protecting myself from further attack?
- How do we define "trust" when businesses increasingly rely upon 3rd parties in the delivery of core products and services? The fingers on the keys in global commerce networks are there on their own local vetting standards unrelated to the security interests of the interdependent players. Owing to the short-term legal commitments to share information, who is a "knowledgeable insider"?
- Are we all very certain that all the trillions of lines of computer code touched in some direct way by thousands of unknown, unvetted individuals in preparing for Y2K are OK?
- The computer hacker and cyber terrorist operating alone, equipped with a PC and modem, inflicting the scope of damage that was previously the realm of organized, well-resourced groups. The technical complexity and uncontrolled interdependencies of global IT infrastructures provide soft targets to sophisticated and unsophisticated adversaries alike.
- InfoWar is considered a plausible national threat and financial service is either a direct target or would suffer serious collateral damage.

I do not want my remarks to give inadequate airtime to the far more frequent and conventional threats of international organized crime, extortion and corrupt practices; money laundering and serious fraud; risk to business in unstable, high threat regions; product counterfeiting or trade secrets compromise. We deal with these in our own ways every day. But, candidly, if we could

find ways to deal with the threats of the future, the results would show immediately in these more conventional and persistent areas. Moreover, most, if not all, of these criminal elements are now using information technology to facilitate their operations.

While each of America's business sectors would likely have its own unique expectations of a security environment, we all share an increasingly interdependent set of threats, vulnerabilities and core concerns. High on the list of expectations is the ability to obtain qualitative, timely and actionable information essential to the protection of our enterprises. This expectation applies to business as well as government. If my competitor is today's victim, I am the likely target tomorrow.

This need for information has played center stage in the 1996-97 work of the Commission on Critical Infrastructure Protection and the related objectives of Presidential Decision Directive (PDD) 63 in 1998. The PDD addresses an approach to the compelling need for more dialogue and information sharing; protocols between government and business. In that same year, when representatives of the G8 assembled to discuss solutions to critical global issues, responding to international financial crime was at the top of their agenda. Not surprisingly, multilateral cooperation and information exchange also emerged as key elements in future strategy. In addition, the G8 recognized the central role of transnational businesses and called for closer public-private cooperation to agree on a legal framework for obtaining, presenting and preserving electronic data as evidence while maintaining privacy protection. Frankly, just about everyone who has thought about cybercrime and cyberwarfare acknowledge that countering the threat requires proactive information sharing between public and private sectors on an unprecedented scale. Over time, this simply cannot be an ad hoc play if I want game.

While we might speculate on the life expectancy of PDD 63 as we enter an election year, I am starting to see some

movement on the dialogue and potential benefits its objectives represent. I also see real multi-jurisdictional action on money laundering within the G8. However, I find myself honestly wondering if either the public or private sectors are ready to seriously work to eliminate the barriers to the essential, risk-based information sharing that will be required in the future. Notable quotes following the recent Internet attacks are instructive of the future challenge:

Commerce Secretary William H. Daley told reporters after the meeting that the government's role was to support the industry and that companies were properly taking the lead in enhancing security.

The industry participants spoke regularly and politely about the need for a continuing partnership with the government in improving [computer] security. But their concept of what role the government would or should have was decidedly limited.<sup>1</sup>

In terms of real consequences, this attack was light skirmish but it did serve to focus attention on future threat and the expansiveness of the potential crime scene. I think an important outcome was to highlight the clear interdependence of corporate victims and public law enforcement. Successful investigation of cybercrime depends significantly on the active collaboration of multiple public and private entities, frequently in different countries.

If we don't collaboratively work on a collective knowledge base, we will never get to solutions on countering these inevitable threats. We must recognize that future risk will challenge the traditionally compartmentalized structures of the national security apparatus and effective response to new threats will require business to redefine the limits of collaboration with government, particularly regulators and law enforcement. As we wait to see the direction of public policy, we in business will continue to allocate significant resources to improving our proprietary control environments as a cornerstone of our fiduciary responsibility to our shareholders.

So, recognizing that thoughtful government-sponsored forums have arrived at some consensus on threat and planful response, the work has to be around some new paradigm of information sharing and joint planning on protection measures. How will we achieve real progress here? What might a few expectations of mine be in this debate?

1. We need timely, reliable and comprehensive information on how appropriate international and domestic intelligence on families of threat and vulnerability adds up to knowledge we should have within established protocols. This is both a business-to-business as well as a bilateral government-to-business issue.

2. We need bilateral trusted relationships with the government agencies upon which we will increasingly have to rely for actionable risk information as well as appropriate and qualitative first response. I'm not sure if this is the chicken or the egg to number one.

3. Perhaps most critical to us, we need to know that there are reliable processes for incident reporting that will assist others' awareness while protecting our corporate privacy and reputation in the marketplace. This is a particularly difficult arena where trust among competitors and the government is paramount. In our early efforts to structure information sharing venues, many of us have agreed to share anonymously among ourselves but have elected to withhold from government. What is the motive for this reluctance?

- Law enforcement and prosecutorial response to our victimization is totally unpredictable. Moreover, in the more technological risks, there is a steep learning curve yet to be met by these agencies.
- We simply do not know what politically motivated interests might do with the information.

- Our prior experience suggests that the process will invariably be a one-way street, and
- Yes, I absolutely could say the same things for a competitor but I have more information to support conclusions that have some real skin in the game and admissions that they may be next.

4. The Departments of Defense and Energy as well as others contributed significantly to the state-of-the-art in physical and logical protection over the past 50 years. This engine of innovative research and development in safeguards should be refreshed and encouraged to find new and cost-effective ways to protect our infrastructure and assets. Security technology is an enabler that can help American business be more competitive.

I believe the balance of power in the source of information on threat and technical response is shifting, perhaps not as subtly as we might think. Business security risk and national security risk are morphing. There are no oceans or mountains to conquer in the virtual landscape. Whether state-supported or individually motivated cyber-terrorists, international organized crime, the knowledgeable insider or unknown individuals masked behind a cyber probe, private enterprise is on the preferred target list. As a result, we in corporate security are becoming increasingly sophisticated, knowledgeable, and equipped on a whole new family of credible threats and effective countermeasures. While I'm here preaching for a new paradigm of public-private information sharing, I will tell you that, on a daily basis, I learn more from my private sector colleagues around the globe than anything I hear from the governments who provide the protective shell around our "domestic" business environment.

Why is that? Is it a clearance thing? Some sort of legitimacy that comes from a public agency vetting process? If so, fine, let's get on with it. If not, we should establish a public-private joint effort to identify the constraints to real

information sharing and identify ways to overcome these barriers to risk-based collaboration. Somewhere out there, right now, the bad guys are sharing information far better than we are. Someday, in the midst of crisis, we may have to find ways to share real information essential to both our interests. It is encouraging to note that after PDD-63 was issued, some highly relevant private sector and government sharing efforts were initiated. I am most familiar with the Financial Services Information Sharing and Analysis Center (FS/ISAC) of which my organization is a charter member, but similar efforts are underway in other infrastructure sectors. The FS/ISAC first seeks to solve the nontrivial problem of facilitating information sharing among competing financial services firms and as noted earlier, we believe that, for now, anonymous information submission is the key to making this work. Once that is working well, the FS/ISAC will look for ways to share information with other sector ISACs. Bi-directional sharing with the government is also a high priority objective expected to evolve over time as trust and appropriate protocols can be developed. This ISAC work is one good example of the kind of mechanisms that I think we need to define and nurture as cornerstones for the improved public-private security relationship of the future. I would add that the finance and banking sector appears to be significantly ahead in the discussion and development of the structures proposed in the Presidential Directive.

I had hoped to be encouraged by the action steps emerging from the 2000 National Planning Retreat sponsored by the Critical Infrastructure Assurance Office (CIAO) several weeks ago in Washington. Three of the agenda topics recognize the overall concerns I have attempted to underscore in my remarks:

- Interdependency Vulnerability Assessment;
- Information Sharing, Awareness, and Education;
- Organization Issues and Public-Private Cooperation.

Aside from highlighting what is *not* happening, it is unclear to me what will come out of this effort to marshal initiative and really move the agreed-upon agenda off square one.

Instead of reinventing the wheel, I would commend the State Department Overseas Advisory Council (OSAC) as a working public-private model of real trust and information exchange. Given the transnational corporate membership of this organization, perhaps other agencies should consider leveraging this entree to substantive information exchange on risk. The International Security Management Association (ISMA), for example, within which I serve as a member of the Board of Directors, actively participates with OSAC and represents the global security interests of the 250 largest transnational firms. Throughout our history, we have looked to our government to define the terms of national security and provide for the means to assure it. A case may be made that those terms are now more defined around a private sector assessment of financial markets and the pivotal U.S. role in the global economy. If that is so, then U.S. business has no choice but to play a larger, more front line role in providing for the "common defense." Our stakehold is as a target of preference with potentially significant consequences, not only for our shareholders, but for the economies to which we are all increasingly tied. In recognition, we operate early warning systems and have a fiduciary responsibility to deploy an effective response to threats against us.

Business and government are too often moved to real action by crisis. We all know the ground has changed and we need to get on with the business of finding ways to manage future risk. Bilateral communication is a keystone. It is in the far too infrequent forums such as this that collaborations will be formed and solutions found.

## CHAPTER 4 - ENDNOTE

1. "Internet Executives Reassured After White House Meeting," *New York Times*, February 16, 2000, p. C2.



## CHAPTER 5

### BALLISTIC AND CRUISE MISSILE THREATS

Steven A. Cambone

I will discuss ballistic missile threats to the United States posed by countries with extant and emerging capabilities, and will raise some questions regarding the strategic implications of these threats for the United States in coming years. I will address cruise missile threats only briefly, as they are, at present, not as pressing a problem in strategic terms as the ballistic missile threat. I will first discuss extant ballistic missile capabilities. Second, I will consider emerging threats and examine the program supporting efforts to develop long-range ballistic missile capabilities in a number of countries. Finally, I will turn to strategic implications of the evolving ballistic missile threat.

#### Extant Capabilities.

Seven countries now have, or have access to, the technology to develop long-range ballistic missile capabilities: Russia, China, North Korea, Iran, Iraq, Pakistan, and India. At least three, perhaps four, countries currently have the capabilities to threaten the United States with ballistic missiles. Russia, China, and North Korea have the ability to place weapons of mass destruction (WMD) on U.S. territory.<sup>1</sup>

There is a lively debate over whether the fourth, Iran, has that capability at present. Open-source intelligence estimates suggest that North Korea has provided substantial assistance to Iran's ballistic missile programs.<sup>2</sup> If North Korea could, as those intelligence estimates indicate, launch its *Taepo Dong 2* in a two-stage configuration carrying a light payload and strike the West

coast of the United States, and in a three-stage configuration strike the entire United States, it likely follows that Iran could possess a missile of a similar range in a relatively short time following a decision to develop it.<sup>3</sup> A three-stage *Taepo Dong 2* would give Iran the ability to target the northeastern part of the United States.

Iraq and Pakistan are two additional countries that give rise to concern. In December 1989 Iraq launched a three-stage rocket capable of putting a satellite into orbit.<sup>4</sup> The rocket exploded after launch, and luckily the overhead Defense Support Program (DSP) satellites detected the launch. But this indicates that, at a minimum, the Iraqis have the interest and desire to acquire such capability. The Rumsfeld Commission assessed that if U.N.-imposed controls were lifted and Iraq mounted a "determined effort," it could pose an intercontinental ballistic missile (ICBM) threat to the United States within 5-10 years.

Pakistan may not have an interest at present in investing in missiles of ICBM range, and it is difficult to imagine the need for this capability arising and therefore posing a direct risk to the United States. Recent press reports and unclassified intelligence estimates indicate that Pakistan's ballistic missile program is closely linked to that of North Korea, which at the very least means that Pakistan likely has access to the technology for long-range ballistic missiles.<sup>5</sup>

India is the last of the seven countries with the current potential to develop ICBM range capabilities.<sup>6</sup> However, I am not including India in the threat calculus, as India is not a country that appears to wish harm to the United States or to its interests. Nonetheless, India's little noted program is moving, with Russian assistance, toward development of SS-20 class ballistic missiles and submarine launched ballistic missiles.

## Program Development.

It is important to note that ballistic missile development programs, in all countries to include the United States, are not wholly indigenous.<sup>7</sup> This is a field of development that has been the subject of a great deal of trade, and exchange of personnel, scientific information, materials, and technologies. Moreover, for a host of reasons, countries have been more than willing to provide assistance to one another, even when one might not think it to be in their interest to do so. Not only has Russia provided submarines, destroyers, and aircraft to China, but also they have provided substantial technical assistance to China's missile and weapons programs.<sup>8</sup> While Russian-Chinese relations were frosty during the 1970s and 1980s, it is worth recalling that the currently deployed Chinese long-range missile force is largely derivative of Russian capabilities that were transferred in the 1950s and early 1960s.

In turn, the Russians and the Chinese have been helpful to many other countries, including Iran, Iraq, North Korea, and Pakistan, both in terms of technology and personnel.<sup>9</sup> The reasons behind their activity are a matter of speculation; the fact remains that entities in both countries are supplying a substantial amount of aid and assistance.

In addition to Russian and Chinese transfers, the trade and assistance among emerging ballistic missile powers is proving to be an extremely troubling trend. North Korea has provided aid to Pakistan and Iran, and India has assisted other countries as well.<sup>10</sup> Thus, even if the Russian and Chinese aid to other countries stopped right now, a sufficient amount of capability is extant in these emerging, second tier countries that their programs would be able to move forward. Development might be slightly slower, more expensive and technically risky, but the programs would advance nonetheless.

The above brief discussion of the military-technical dimension of the threat is what most frequently draws our

attention. The last part of the chapter will raise some issues of a strategic dimension to inform the deployment decision.

### The Strategic Dimension.

We have comforted ourselves with the knowledge, or what we believe to be the knowledge, that Russia's strategic offensive forces are going to be very small, relatively speaking, in the near future.<sup>11</sup> Some suggest that the ultimate number will be on the order of 1,000 warheads, though I would argue that this is doubtful. In any event, the number will be somewhere between the 3,000 or so that are permitted under Strategic Arms Reduction Treaty (START) II and whatever we may negotiate under START III. However, it is important to appreciate that those forces are going to be far more modern than the forces the Soviets deployed in the 1980s. The SS-27, Russia's new ICBM, is a very good piece of work, and the missile it is now putting together to deploy on their follow-on submarines will likely be just as advanced. Moreover, the Russians have indicated that they hope to use this new sea-launched ballistic missile (SLBM) as a common missile for both the land and sea-based deployments.<sup>12</sup> It is worth noting, in addition, that while the SS-27 is being deployed as a single warhead missile, it is perfectly capable of carrying more than one re-entry vehicle. Thus, while there will be fewer delivery vehicles, the Russians will have the potential to maintain a fairly large number of warheads in the force.

China, on the other hand, is the only nuclear weapon state committed to building up its offensive potential.<sup>13</sup> Its forces in the next 10 to 15 years will be far larger than they are today. The unclassified intelligence estimates indicate that, in addition to their land-based CSS-4's, China will have some "few tens" of additional land-based and sea-based ballistic capabilities.<sup>14</sup> In addition, while the current model of the land-based system could carry maneuvering reentry vehicles (MaRVs), the follow-on systems to the DF-31, now in testing, to include the SLBM

variant, are projected to have much more throw weight and could carry MIRVs (multiple independently targeted reentry vehicles) and have an 8,000 km range. The DF-31 was tested in August 1999, and unclassified U.S. intelligence sources suggest that deployment may be near but has not yet happened.<sup>15</sup> The follow-on to the DF-31 is projected to have a range of 12,000 km.<sup>16</sup> Thus, the Chinese are going to have a much larger force and one of fairly reasonable strategic potential in the next 10 years or so. This potential is of interest, particularly when you realize that our own force capabilities are coming down in total numbers and in the number of targets the force presents.

With regard to the emerging ballistic missile powers, their activity is not ad hoc; it is not taking place outside the purview of the leadership. Rather, their missile development and related proliferation activity is being conducted with specific political and strategic purpose. One need only consider the long-standing relationship between China and Pakistan relative to Russia and India to begin to identify potential strategic purposes. To cite another example, it is difficult to understand Russian activity with Iran in any other but a political and strategic context.

### Strategic Implications.

Next, I would like to raise some of the strategic implications related to ballistic missile development, and how these implications might affect our own calculations about our position in various regions around the world.

It is instructive to examine what countries might gain by the development of ballistic missile programs. North Korea, I would suggest, gains *recognition*. North Korea has engineered a direct relationship with the United States, a summit with South Korea, and an opening to other Asian and European states—it is now received in Canberra, Rome, Paris, and Geneva—all made possible by the existence of this recognition. Whether or not this is precisely

what North Korea had in mind when beginning its programs, it is certainly making use of that recognition.

Iran, in my view, is seeking *reintegration* through its missile development. At the very least, this is one of the consequences of its programs. We have seen “pistachio diplomacy” unfold, an effort by the United States to develop favorable relations with the reform-minded Khatemi government. This U.S. effort comes despite the lack of any evidence that the Khatemi government is willing to alter substantially or abandon its programs. Iran has also opened dialogues with European states and with its Gulf Cooperation Council neighbors, especially Saudi Arabia.

India is seeking *admission*; I would argue it has wanted a seat at the table in discussions of regional and world affairs, and has achieved one, even if it is still present via conference call, if you will. One need only recall that the President visited India for 5 days in mid-2000—he visited Pakistan for 5 hours.

Pakistan, in contrast, hopes for *leverage*. More than just the status of possessing long range missiles, they seek leverage over the problem with India, and thus far have failed to gain it.

Iraq, I would argue, is looking very hard to *reconstitute* its society and position in the region, and my guess is that, in the course of this, they will reconstitute their weapons capability as well.<sup>17</sup>

These are the so-called bad guys, the rogues. Whatever the latest State Department preferences, “rogue” is a word that we should ban from our lexicon. These are countries that have specific strategic intentions, and they have set out to achieve them. Addressing the implications of their intentions begins by respecting their threat.

Allies.

Our allies have much to come to grips with as a result of missile developments. After a North Korean launch of the *No Dong* missile over its territory, Japan decided it would do two things: first it would join the United States in its theater missile defense (TMD) program.<sup>18</sup> Secondly, and more significantly, it decided to go ahead with its own satellite reconnaissance program.<sup>19</sup> The importance of this decision lies not in the constitutional implications for Japan, or that it is militarizing space, but rather in the notion of the "tyranny of information." The Japanese leadership is no longer going to depend upon the United States for information about what is taking place in its backyard. With this information, however, comes responsibility. The Japanese leadership can no longer duck the Japanese public's questions about potential threats or ignore calls for responses.<sup>20</sup> Thus, as a consequence of responding to this missile threat, Japan is going to have more information about what is taking place in the region, which will, in turn, increase the requirement for action by the public. This will dovetail, I believe, with what one already sees as a generational change in the attitude of the Japanese about their role in the region.

South Korea, too, has designs on a changed role in the region, which has its strategic implications. The United States has tried very hard to convince South Korea to buy theater missile defenses, but to no avail. The South Koreans believe that to defend themselves properly, they need a deterrent capability such as the United States has against the Russians, which means offensive potential. While they are happy for the United States to bring theater missile defenses with the U.S. troops deployed on the Korean peninsula, they want 500 km-range ballistic missiles with which to attack the launch sites in North Korea. This is not inconsistent with South Korea's effort to bring a rapprochement with the North. However, since 1990, missiles of a range exceeding 180 km have been prohibited

by an agreement between the United States and South Korea. According to press reports, these restrictions have been expanded to 300 km for payloads up to 1,100 pounds and longer for lighter loads.<sup>21</sup> This development could have significant implications insofar as South Korea will, in effect, be a member of the Missile Technology Control Regime (MTCR) club and, in turn, could gain access to the kinds of technological capabilities which would support what they consider to be their real objective: a space launch capability. This does not need to be spun out further to clearly see the strategic implications of now three countries in the region armed with ballistic missiles.

Taiwan finds itself in a difficult position, which has been exacerbated by the ballistic missile threat.<sup>22</sup> China understands that ballistic missiles can have the same effect as navies once did; that is, a force with which to coerce and to conduct the modern day equivalent of gunboat diplomacy.<sup>23</sup> This is no small accomplishment and one the United States needs to address. The Taiwanese are not sure how they are going to deal with this problem, and they are worried also about the relationship with the United States in light of China's threats and ballistic missile modernization program.<sup>24</sup>

Saudi Arabia's prince and defense minister went to the nuclear and ballistic missile facilities in Pakistan, most likely for the same reason that Saudi Arabia acquired the CSS-2 back in 1988: they are nervous about developments in their area of the world.<sup>25</sup> Saudi Arabia can be reached or threatened with ballistic missiles by India, Pakistan, Iran, Iraq, and Israel. If the Saudis are going to play in the regional military balance, they likely will need to replace the CSS-2s. This is a momentous decision for Saudi Arabia, and one that is going to be extraordinarily important for its effect, in turn, on the delicate political balance in the region.

Finally, Israel is in the midst of an agonizing reappraisal, the kind John Foster Dulles once spoke of. Israel understands that Iran now threatens it in ways that



it has never been threatened before. The Israeli's defense forces—particularly its ground and air forces—can no longer provide the unqualified strategic deterrence or defense for Israel. The enemy, should Iran prove to be such, is no longer contiguous, and not able to be touched in the way that Israel did when it destroyed Iraq's nuclear reactor at Osirak. Thus, we see a flurry of activity by the Israelis. They are looking to make peace to the north with the Syrians, and it is not improbable that they could open a dialogue with the Iranians as well.<sup>26</sup> Israel and the Shah's government maintained good relations, and there is a long history of relationships between those two countries. In addition to the diplomatics, the Israelis are also rethinking the approach their strategic forces should take. It is not coincidental, I would argue, that according to press reports, the Israelis are looking for Tomahawk Cruise missiles, perhaps to arm either surface ships or, more likely, the submarines that they are acquiring.<sup>27</sup> If Israel arms itself with cruise missiles, the lid will be off the box, and the United States will have an additional set of technical capabilities in the mix that might have the effect of destabilizing the region. This is not to argue against the Israelis acquiring these missiles, but rather for the need to be aware of the likely consequences.

## Conclusions.

First, technical development of the ballistic missile threat is difficult to control. While one should never give up the effort to conduct anti-proliferation measures, we have to realize that we will only slow the programs, not end them. Second, there are now multiple centers of ballistic missile capability and we are going to have to keep them all in mind as we think through our arms control approach, our missile defense process, and the development of our armed forces capabilities over time. Third, it is important to remember that those centers do cooperate technically. It would not be surprising to discover that they also develop political or strategic alliances of convenience as time goes by. This is

perhaps not unlike the alliance of convenience between the Russians and the Chinese or the North Koreans and the Iranians. The United States must keep this cooperation in mind as we weigh the risks and choose a course of action in potential developing crises; a crisis in the Middle East might have reverberating effects as far away as Northeast Asia. Lastly, it seems that proliferation of ballistic and nuclear, biological, and chemical technologies, and in some cases the actual deployment of the systems, underscores not only the increased instability of the international system, but also the present inability of the United States to negate the use of those systems.

## CHAPTER 5 - ENDNOTES

1. "Foreign Missile Developments and the Ballistic Missile Threat to the United States Through 2015," National Intelligence Council Report, September 1999 (hereafter NIC Report); "Commission to Assess the Ballistic Missile Threat to the United States," Pursuant to PL-201, July 15, 1998, (hereafter Rumsfeld Report).

2. See Statement of Director of Central Intelligence George J. Tenet before the Senate Foreign Relations Committee, March 21, 2000. For reports in the press, see "Critical N. Korea Missile Parts Seen Aiding Iran's Program," Bill Gertz, *Washington Times*, February 10, 2000; and "N. Korea Sells Iran Missile Engines," *Washington Times*, February 9, 2000. Also see "Israel Preparing for Iranian Test Launch of Shahab 3 Missile in Coming Weeks," *Tel Aviv Ha'aretz*, June 26, 2000, translated in *Foreign Broadcast Information Service* (hereafter FBIS).

3. NIC Report.

4. "U.S. Confirms Iraq Has Launched Rocket That Can Carry Satellites," Michael Gordon, *New York Times*, December 9, 1989.

5. "U.S. Says North Korea Helped Develop New Pakistani Missile," Tim Weiner, *New York Times*, April 11, 1998; and, "Pakistan Raises Artillery Unit to Handle Long Range Missiles," Mumbai, *The Times of India*, June 26, 2000, in FBIS

6. This point is made in David R. Tanks, "Ballistic Missiles In S. Asia: Are ICBMs a Future Possibility?" in Appendix III, Unclassified Working Papers for the Rumsfeld Commission. See also "Indian Missile Programme" *Asian Defense Journal*, May 1995, p. 20.

## 7. NIC Report.

8. On conventional assistance, see "Chinese Raises Arms Stakes with \$500 Million Destroyer," Tyler Marshall, *Los Angeles Times*, February 2, 2000; and "Sino-Russian Arms Sale is Reaching the Second Stage in 2000," *Kanwa News*, January 20, 2000, [www.kanwa.com](http://www.kanwa.com) (visited June 24, 2000). For reports of nuclear assistance, see "Report to Congress on Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions: January 1, 1999 to June 1, 1999," required pursuant to Section 721 of FY 97 National Intelligence Authorization Act, 9 (hereafter China Report), and "Inside the Ring: Beijing-Moscow Axis," Bill Gertz and Rowan Scarborough, *Washington Times*, January 14, 2000.

9. See "China, Russia Still Exporting Nuclear, Missile Technology," Bill Gertz, *Washington Times*, February 2, 2000. See also China Report, note 10.

10. See Testimony of Director of Central Intelligence George Tenet before the Senate Foreign Relations Committee on "The Worldwide Threat in 2000: Global Realities of Our National Security," March 21, 2000. Available at [www.cia.gov](http://www.cia.gov) (visited June 26, 2000).

11. NIC Report. See also report of statement by Russian Chief of General Staff Anatoly Kvashnin, "Russian CGS Thinks Russian Strategic Arsenal Must Be Cut," *Moscow Interfax*, June 24, 2000, translated in *FBIS*.

12. "Russian Admiral Vaunts Naval Missile Systems," *Interfax*, January 4, 2000, translated in *FBIS*. See also "Center TV Carries Interview with TOPOL M Designer," *Moscow Center TV*, December 17, 1999, translated in *FBIS*.

13. "China, Nuclear Weapons, and Arms Control: A Preliminary Assessment," Brad Roberts, Robert A. Manning, and Ronald Montaperto, published by the Council of Foreign Relations in conjunction with National Defense University, and the Institute for Defense Analyses, 2000. See also "U.S. National Security and Military/Commercial Concerns with the People's Republic of China," Vol. I, Select Committee of U.S. House of Representatives, 1999 (Cox Report), and "Annual Report on the Military Power of the People's Republic of China," Pursuant to Section 1202 of the FY2000 National Defense Authorization Act. See also James R. Asker, "Determined to Build," *Aviation Week and Space Technology*, May 15, 2000.

14. NIC Report; James R. Asker, "Determined to Build," *Aviation Week and Space Technology*, May 15, 2000.

15. On the flight test, see "China Develops Warhead Decoys to Defeat United States Defenses," Bill Gertz, *Washington Times*, September 16, 1999. A PLA daily newspaper quoted in *Jane's Defense Weekly* states that the missile has already been deployed. See "China Deploys Dong Feng 31 Missile Towards Its Southern Borders," Yihong Zhang, *Jane's Defense Weekly*, November 2, 1999. On United States sources, see the Cox report and "China: The Forgotten Nuclear Power," Brad Roberts, Robert A. Manning, and Ronald Montaperto, *Foreign Affairs*, July 2000.

16. "NMD: An International Concern" *Jane's Intelligence Review*, May 1, 2000, Vol. 12, no. 5, and Brad Roberts, Robert A. Manning, and Ronald N. Montaperto, "China: The Forgotten Nuclear Power."

17. Press reports confirm that this is the case. See "Flight Tests Show Iraq has Resumed a Missile Program," Steven Lee Meyers, *New York Times*, July 1, 2000.

18. "U.S. and Japan Agree to Joint Research on Missile Defense," Calvin Sims, *New York Times*, August 17, 1999.

19. "North Korean Missile Threat is Reassessed: 3 Stage Rocket Was Not Foreseen by United States," Bradley Graham, *The Washington Post*, September 25, 1998; "Need Seen for Spy Satellite," Michiyo Nakamoto, *Financial Times*, September 9, 1998; "U.S. and Japan Agree to Joint Research on Missile Defense," Calvin Sims, *New York Times*, August 17, 1999.

20. "Japan Moves Towards a New Assertiveness: Sense of Insecurity and Crisis Prompts Lawmaker and Public," Cameron Barr, *Christian Science Monitor*, July 8, 1999.

21. "As Relations Thaw, Seoul Suspends Arms Plan," Doug Struck, *The Washington Post*, June 25, 2000. This article stated that Seoul had put their missile program on hold in light of the recent summit, though this was denied by officials in the Korean Foreign Affairs and Trade Ministry. See "ROGK Denies United States Daily Report of Canceling Longer-Range Missile Development Plan," *Seoul Yonhap*, June 26, 2000, translated in *FBIS*.

22. "China may Build Arms to Gain Edge on Taiwan," Eduardo Lachia, *Wall Street Journal*, June 26, 2000.

23. "China's Missile Tests Reveal a Potential United States Can't Ignore," Sheila Tefft, *Christian Science Monitor*, March, 26, 1996.

24. In the wake of the apparently successful Korean summit, President Chen Shui-bian invited Jiang Zemin to meet. See "Taiwan's President Calls for Summit With China," John Pomfret, *The Washington Post*, June 20, 2000.

25. "Saudi Visit to Arms Site in Pakistan Worries U.S." Jane Perlez, *New York Times*, July 10, 1999.

26. On both Israeli government and military support for a peace deal with Syria, see "Israel War Games Boost Peace Talks," Sam Kiley, *The London Times*, January 14, 2000.

27. "U.S. Nixes Israel Tomahawk Plea, Could Spur Indigenous Development," Barbara Opall-Rome, *Defense News*, March 20, 2000.

## CHAPTER 6

### CHEMICAL AND BIOLOGICAL TERRORISM: POLITICAL HYPE OR BONA FIDE POST-COLD WAR THREAT?

Russell Howard

America's current national security structure is based on the National Security Act of 1947. That legislation was enacted to correct coordination and operations deficiencies observed during World War II and to facilitate efforts to address the emerging Soviet threat. For the most part, as noted by President Clinton on the 50th anniversary of the Act, it has worked:

The success of their efforts and of the historic legislation enacted half a century ago is reflected in an outstanding record of achievement: nuclear war averted, the Cold War won, and the nations of the world turning to democracy and free markets.

However, many question whether the Act and the institutions and treaty regimes it created are equal to the challenges of post-Cold War global security. In these critics' opinion, the 1947 document was adequate for a bipolar, state-centric, balance-of-power world, in which the Soviet Union was the enemy and interstate conflict the main threat. But, they view it as inadequate for the unipolar, less state-centric, post-Cold War world, in which our principal enemies are failed, failing, and rogue states and transnational actors. Now the principal threats are ethnic and religious conflict, international and domestic terrorism, drugs, and the proliferation of weapons of mass destruction (WMD).

This chapter contends that the critics of the National Security Act are right, especially regarding the proliferation and use of two types of WMD—chemical and biological—in

the United States and internationally. It begins by reviewing the debate over the seriousness of the chemical/biological weapons threat to U.S. security. It considers the limitations of the 1947 Act and discusses how the United States is presently organized to address threats from such weapons, arguing that a streamlined organizational structure under unitary command would be more efficient and timely. It examines how the United Kingdom, Canada, and Israel are organized to handle chemical and biological threats to their homelands and suggests that the United States has much to learn from these important allies.

The chapter also discusses certain intelligence reforms that may be necessary to help curtail the use of biological and chemical weapons by terrorists. It identifies some limitations of the Posse Comitatus Act, which severely curbs the use of U.S. military forces against domestic acts of chemical and biological terrorism. Finally, it analyzes the viability of deterrence and preemption as means of preventing the use of such weapons in the future.

### Chemical and Biological Weapons in History.

The problem of chemical and biological weapons is not entirely new. The use of mustard gas during World War I is well known, but other examples go back much further. "Toxic fumes" were used in India as early as 2000 BC. The first known use of biological warfare was in 1346 at Kaffa (now Fedossia, Ukraine), where the bodies of Tartar soldiers who had succumbed to plague were catapulted over the walls of the besieged city.<sup>1</sup> During World War II the Japanese produced biological weapons and used them in 1942 at Congshan, China—the only confirmed air attack with biological weapons in modern history.<sup>2</sup> A recent book, *The United States and Biological Warfare: Secrets from the Early Cold War and Korea*, charges that, after World War II, the United States used knowledge acquired by the Japanese to develop a lethal biological arsenal, which was tested in

Korea and China during the Korean War.<sup>3</sup> Iran used chemical weapons during the Iran-Iraq War, perhaps even on its own citizens.<sup>4</sup> Iraq's chemical weapons stockpile and suspected production facilities have motivated United Nations inspections and U.S. missile and air strikes for years. The United States believed that the Serbian army had stocks of lethal chemical weapons, which might be used against the Kosovars.<sup>5</sup> The Center for Nonproliferation Studies at the Monterey Institute of International Studies has identified 31 states that have or had chemical or biological weapons programs and have catalogued at least 46 instances of their use.

### A Serious Post-Cold War Problem.

At present there is a debate among analysts and scholars about the severity of the threat posed by WMD, especially biological and chemical weapons. The Hart-Rudman Commission argues in a 143-page report that the most serious potential threat to the United States may be unannounced attacks on American cities by terrorist groups using germ warfare.<sup>6</sup> The report predicts that "Americans will likely die on American soil, possibly in large numbers."<sup>7</sup> The growing threat of domestic terrorism is one of the leading themes of this study, which Secretary William R. Cohen has called the most comprehensive effort of its kind since the National Security Act of 1947.<sup>8</sup> Cohen agrees that WMD threats are extreme:

I believe the proliferation of weapons of mass destruction presents the greatest threat that the world has ever known. We are finding more and more countries that are acquiring technology—not only missile technology—and are developing chemical weapons and biological weapons capabilities to be used in theater and also on a long-range basis. So I think that is perhaps the greatest threat that any of us will face in the coming years.<sup>9</sup>

Others disagree. Milton Leitenberg, a senior fellow at the Center for International and Security Studies at the



University of Maryland considers the Secretary's comments exaggerated and alarmist. According to Leitenberg, no agency of the U.S. Government has prepared a threat analysis indicating that the use of chemical and biological agents by terrorists is imminent or even likely. Rather, "various analysts have provided vulnerability projections and scenarios, which are always easy to concoct in the abstract."<sup>10</sup> So far, Ehud Sprinzak points out that the world has not witnessed any mass-casualty event resulting from unconventional terrorists using WMD. "Most of the funds allocated to countering this threat have been committed on the basis of dubious conjecture and unsubstantiated worst-case scenarios."<sup>11</sup> Brian Jenkins notes that of the eight thousand terrorist incidents recorded between 1968 and 1986, fewer than 60 offered any indication that terrorists considered using chemical or biological agents.<sup>12</sup> Nicholas Wade of the *New York Times* argues that biological weapons are too difficult to disperse to be technically feasible for other than the most sophisticated users.<sup>13</sup> Like most other people, terrorists fear powerful contaminants and toxins about which they know little and which they are uncertain how to fabricate and handle, much less deploy and disperse.<sup>14</sup> "Few countries," writes Jessica Stern, "and even fewer terrorist groups, if any, are now capable of launching an open-air attack that would create mass casualties."<sup>15</sup> Brian Jenkins's often-repeated observation—"terrorists want a lot of people watching, not a lot of people dead"—seems to imply that terrorists are unlikely to resort to WMD."<sup>16</sup>

Use of chemical and biological weapons by terrorists has indeed been rare. One recent exception was the Aum Shinrikyo sarin gas attack on the Tokyo subway; and those involved in the 1993 World Trade Center bombing were gathering the ingredients for a chemical weapon that could have killed thousands.<sup>17</sup> There were 68 investigations into the threatened use of chemical, biological, or nuclear materials in the United States in 1997, and 86 in the first 9 months of 1998, but all turned out to be hoaxes.<sup>18</sup> The only

significant case of bioterrorism in the United States occurred in Oregon in 1984, when followers of Indian guru Bhagwan Shree Rajneesh, hoping to sway a local election, unleashed a salmonella poisoning attack in ten restaurants, sickening 751 people but killing none.<sup>19</sup>

Nevertheless, though WMD attacks have so far been extremely rare, there are several reasons why this threat must be taken seriously. First, such attacks have the potential to be unprecedentedly devastating—the United States simply must be capable of preventing them or responding swiftly and efficiently if prevention fails. Second, advances in information technology and the increasing availability of ex-Soviet WMD specialists have made the fabrication and use of biological and chemical weapons a less intimidating prospect for terrorists. Third, there are now many terrorists who do not adhere to Brian Jenkins's dictum—they do want to "see a lot of people dead."

Chemical and Biological Weapons—One Horrible, the Other Worse.

Chemical and biological agents are not always distinguished in popular discourse, but there are important differences between them. Agents used in biological weapons are "living organisms or infective material derived from them, which are intended to cause disease or death in man, animals, and plants, and which depend for their effects on their ability to multiply in the person, animal, or plant."<sup>20</sup> Agents used in chemical weapons are gaseous, liquid, or solid chemical substances which cause death in humans, animals, or plants and which depend on direct toxicity for their effect.<sup>21</sup>

Biological weapons are strategic. They are "incredibly powerful and dangerous. They can kill huge numbers of people if they are used properly, and their effects are not limited to one place or a small target."<sup>22</sup> Biological agents are microorganisms—bacteria or viruses—that invade the body, multiply inside it, and destroy it.<sup>23</sup> They can infect

nonhuman populations as well, upsetting the entire ecosystem. For example, wild rodents living outside a factory in Omutinsk, Russia, became chronically infected with the Schu-4 military strain of tularemia being manufactured there, a bacterium that causes one type of pneumonia. "It was a hot, lethal strain that came from the United States: an American biological weapon that the Soviets had managed to obtain during the nineteen-fifties."<sup>24</sup> Even though rodents are not a natural host of tularemia, Schu-4 sped among the rodents of Omutinsk. People catch tularemia easily from rodents, and it can be fatal.<sup>25</sup>

Biological weapons are more difficult to acquire and manufacture than chemical weapons, but many states and nonstate actors can now construct them.

Culturing the required microorganisms, or growing and purifying toxins, is inexpensive and could be accomplished by individuals with college-level training in biology and a basic knowledge of laboratory technique. Acquiring the seed stocks for pathogenic microorganisms is not particularly difficult.<sup>26</sup>

One expert estimates that more than 20 countries may now have biological weapons capability.<sup>27</sup>

Chemical weapons are poisons that kill after making contact with the skin. They are tactical instead of strategic; they can be used for mass-casualty attacks in confined areas, but it is almost impossible to concentrate enough chemicals in the air to kill a great many people over a large territory. Because chemicals are not alive, they cannot be spread by infection, like biological weapons. But chemical weapons are easier to fabricate than biological weapons:

Chemical weapons suitable for mass-casualty attacks can be acquired by virtually any state and by nonstate actors with moderate technical skills. Certain very deadly chemical warfare agents can quite literally be manufactured in a kitchen or basement in quantities sufficient for mass-casualty attacks.<sup>28</sup>

In fact, chemical agents are so easy to make that several countries have added them to their weapons inventories. According to unclassified military information, there were 11 countries with chemical weapons in 1980—by 1997 there were 25.<sup>29</sup>

Chemical and biological attacks require different responses.

After a chemical attack, there is a 'golden hour' within which to make a difference. After that hour, those who are going to survive, do, and those who are not, do not. Once decontaminated and removed from the incident site, or 'hot zone,' victims can be dispersed to hospitals.<sup>30</sup>

Biological attacks are more difficult to manage.

The victims must be immediately isolated in order to prevent the agent from spreading. Potential victims need to be isolated from the definitely uncontaminated public; they also should be isolated from others afflicted with the illness until each individual's degree of contamination can be established. But this type of quarantine is currently impossible. Given today's detection capabilities and the incubation period of biological agents, we'll never know that we've been contaminated. Hence the diabolical genius of a biological agent attack: we become the "unknowing vector" of our own death.<sup>31</sup>

New Technology and the Russian Connection.

The Internet has been a major factor in providing WMD "how-to" information to would-be terrorists. By accessing any of a number of search engines, one can get the data necessary to build both chemical and biological weapons. There are also a number of self-published manuals available with information on how to grow and distribute biological toxins.<sup>32</sup> One of these manuals, *Bacteriological Warfare: A Major Threat to North America*, is described on the Internet as a book for helping readers survive a biological weapons attack. But in fact it also describes the reproduction and growth of biological agents and includes a chapter on "bacteria likely to be used by the terrorist." The

book is sold over the Internet for \$28.50 and is reportedly advertised on right-wing radio shows.<sup>33</sup>

The availability of material and expertise from the former Soviet Union also makes proliferation more likely. Between 1969, when the United States halted its biological weapons program, and 1992, the Soviet Union developed the largest and most sophisticated biological weapons program in the world. In 1992 Boris Yeltsin wisely declared that biological weapons activities were illegal. But unfortunately his actions also put many people out of work.<sup>34</sup> Now hundreds and perhaps thousands of unemployed Russian biological and chemical specialists are available to the highest bidder. Among the bidders are the United States, the United Kingdom, Iran, Iraq, and Libya.<sup>35</sup>

## The New Terrorism.

The noted author Walter Laqueur views the “new terrorism” as actually many terrorisms. According to Laqueur,

the past few decades have seen the birth of dozens of aggressive movements espousing varieties of nationalism, religious fundamentalism, fascism, and apocalyptic millenarianism.<sup>36</sup>

Most international and domestic terrorism today is not ideological (in the sense of left or right) but is ethnic-separatist in inspiration . . . In the past, terrorism was almost always the province of groups of militants that had the backing of political forces; in the future, terrorists might be individuals on the pattern of the Unabomber or like-minded people working in very small groups.<sup>37</sup>

According to Secretary of State Madeleine K. Albright:

What's new is the emergence of terrorist coalitions that do not answer fully to any government, that operate across national borders, and that have access to advanced technology.<sup>38</sup>

Such groups are not bound by the same constraints or motivated by the same goals as nation-states.<sup>39</sup> And unlike state-sponsored groups, religious extremists, ethnic separatists, and lone unabombers are not susceptible to traditional diplomacy or military deterrence. There is no state with which to negotiate or against which to retaliate.<sup>40</sup>

No longer are most terrorists concerned about limiting casualties. Religious terrorists, in particular, often seek to inflict many casualties. As Bruce Hoffman observes,

the growth of religious terrorism and its emergence in recent years as a driving force behind the increasing lethality of international terrorism shatters some of our most basic assumptions about terrorists and the violence they commit.<sup>41</sup>

Incidents like the Tokyo subway attack and the World Trade Center and Oklahoma City bombings appear to render Brian Jenkins's dictum about casualties obsolete. Altogether, the availability of Russians for hire and of critical WMD information on the Internet, coupled with the lethal motives of the "new terrorists," could portend a bloody and destructive era for which the United States is ill-prepared.<sup>42</sup>

Overreaction is Not the Answer.

Recognizing the problem is essential, but the United States must avoid overreaction. Achieving total security would be impossible, and it would be tragic for the world's most powerful democracy to abandon any of its freedoms and principles in a quest for absolute security.<sup>43</sup>

Also, attempting to achieve total security would be extraordinarily expensive. And, as the U.S. General Accounting Office (GAO) and others have pointed out, throwing money at it is not the answer. New programs addressing the biological and chemical weapons threat have made counterterrorism one of the fastest-growing parts of the federal budget. Total U.S. spending could exceed \$10 billion in 2000, up from \$5.7 billion in 1996. A report

released in October 1999 by the GAO charges that lawmakers have dumped too much money into this area, and a growing number of government and private counterterrorism experts agree. These experts say:

federal officials are so spooked by the possibility of a chemical or biological attack that they are deliberately hyping the threat to get Congress to cough up coveted cash for prevention programs. And most lawmakers are buying it wholesale.<sup>44</sup>

In 1997, for example, Congress ordered DoD to conduct multi-agency training exercises in the nation's 120 largest cities against WMD attacks. Today there are more than 200 training courses, run not only by DoD but also by the Department of Energy, the Justice Department, the Central Intelligence Agency, the Environmental Protection Agency, and the Federal Emergency Management Agency. Many believe that these programs are redundant, including one over-trained fire-battalion chief who quipped: "Just how many different ways are we going to cook the same chicken?"<sup>45</sup>

### Limitations of the National Security Act.

The National Security Act of 1947, which created the Department of Defense, the United States Air Force, the Central Intelligence Agency, and the National Security Council, was intended to correct coordination and operations deficiencies observed during World War II and to address the emerging Soviet threat. For the most part, it worked. Some may believe that America's military services have yet to coordinate their operations optimally, but no one can deny that joint operations are exponentially better organized today than during the Second World War. As for the Soviet threat, it—like the Soviet Union—no longer exists. What has replaced it is very much diminished; if Russia did not have nuclear weapons it would probably not be considered a major power. Russia today has the same GDP as New Jersey—hardly the basis of a superpower.

The global security environment has changed. No longer does ideology dictate superpower confrontation. No longer do the superpowers and their surrogates compete for the world's allegiance and resources. No longer do realist and idealist theories based on sovereign state behavior and state interaction provide satisfactory frameworks for discussing American and international security. Nowadays failed, failing, and rogue states and transnational actors are our chief security concerns. They are the main sources of the proliferation of WMD, drugs, international and domestic terrorism, transnational crime, ethnic and religious conflict, and other new security threats. The National Security Act was not designed and has not been adapted to address these threats, as events like Somalia, Haiti, Kosovo, East Timor and Oklahoma City attest.

The crucial question is whether the Act and the structure it established can be made to fit the changed national security environment without drastic revision. Some have concluded, like the Center for Strategic and International Studies in Washington DC, that the current structure has sufficient flexibility.<sup>46</sup> Supreme Allied Commander Europe General Wesley Clarke agrees; he sees no need for "big changes" in the Act and believes that it can be adapted to the post-Cold War world.<sup>47</sup>

I disagree. I believe there are two fundamental weaknesses and deficiencies in the National Security Act. First, DoD is not organized correctly. Second, roles and missions within the intelligence community do not support today's requirements.

Department of Defense.

DoD is still organized to respond to major interstate conflict, much as it was during the Cold War. Then it was required to maintain forces for "prompt and sustained combat operations" against the Soviet Union. Though there was always debate about the proper balance of nuclear and conventional capabilities and the most efficient division of



resources among the various services, the defining context—security against a Soviet threat—was relatively unambiguous.<sup>48</sup>

Since the fall of the Soviet Union, the basis for determining the roles, missions, and capabilities of the forces within DoD has been difficult to articulate. Several attempts at redefinition—Bush’s “Base Force,” Clinton’s “Bottom-Up Review,” and the congressionally-mandated “Quadrennial Defense Review and National Defense Panel”—have recommended maintaining a less robust status quo. In essence, the United States has chosen a smaller but heavier version of its Cold War forces, but organized, modernized, and equipped with systems and doctrine appropriate for two simultaneous regional conflicts. Yet except for the Gulf War, our military forces have taken on entirely new missions, such as peacekeeping, peace-enforcement, humanitarian assistance, de-mining, counter-proliferation and counter-terrorism.<sup>49</sup>

The Unified Command Plan (UCP)—related to but not specifically included in the National Security Act—needs to be changed. At present the major regional commands are the European, Pacific, Central (including the Middle East, Persian Gulf, and North Africa), and the Southern (including Central and South America) Commands. The former Atlantic Command is now the Joint Forces Command, which has responsibility for the Atlantic region and additional “joint” responsibilities to the other commands, including training, force integration, and providing trained and ready forces from the United States.<sup>50</sup>

Absent from the UCP is a Homeland Defense Command. Protecting the territory of the United States and its citizens from “all enemies both foreign and domestic” is the principal task of government.<sup>51</sup> The UCP is externally oriented: it protects our borders from foreign enemies. It is not organized to defend the homeland against internal attack by either foreign or domestic enemies. The reason for a

Homeland Defense Command is the change, both in type and degree, in the principal threats to the United States. Besides the continuing requirement to deter strategic nuclear attack, the United States must now also defend itself against information warfare, WMD, terrorist attacks, and other transnational threats to the sovereign territory of the nation.<sup>52</sup> Above all, the security environment has been significantly altered by the proliferation of biological and chemical weapons and their increasing ease of delivery.<sup>53</sup> The complexity of the chemical and biological weapons challenge lies in the huge number of potential enemies who have access to this asymmetric means of attacking the United States in an effort to offset America's conventional and nuclear strength.<sup>54</sup>

An integrated set of active and passive measures for deterring and defending against chemical and biological weapons use is required. These measures must involve a range of federal departments and agencies, which, in turn, must incorporate state and local governments in their planning.<sup>55</sup> Managing the consequences of biological and chemical attacks will also involve all levels of government.<sup>56</sup> Obviously DoD has a significant role to play in these efforts. But what that role should be will be the topic of a later section in this chapter.

The Intelligence Community: We Have Slain the Bear, but There Are Still a Lot of Serpents Around.<sup>57</sup>

The Intelligence Community (IC) is a group of 13 Executive Branch agencies and organizations whose core was established by the National Security Act of 1947.<sup>58</sup> Its mission—to provide an information advantage to those who formulate and execute national policy—has not changed since then, though the nature of the information it deals in has changed markedly. “During the Cold War era, the IC justified its existence by containing Soviet expansion.”<sup>59</sup> Now, however, new missions must be defined if the IC is to maintain legitimacy and focus. Perceived legitimacy has

been a problem, at least for the community at large. Likewise focus: some critics describe the IC as an ad hoc structure in which each agency or organization makes sense individually but which does not function as a well-integrated whole.<sup>60</sup> Even Congress often views the IC as separate voices rather than as a whole.<sup>61</sup>

These problems have prompted an extensive reevaluation of U.S. intelligence by a number of commissions and panels. All these studies, performed by the government or by government-sponsored commissions, have, according to Morton Halperin, “reached the same conclusion, which is that the intelligence structures that we have are just right.”<sup>62</sup> Quips Halperin:

One can only view this as remarkable; here we have a world in which an intelligence community created fifty years ago to fight the Cold War against the Soviet Union turns out to [have] exactly the right set of structures and exactly the right set of functions to deal with this new post-Cold War world.<sup>63</sup>

But suppose, he goes on to ask, that the world really is different? Suppose the IC created 50 years ago is not exactly suited to it? What changes might one make?<sup>64</sup>

Detailed answers to all these questions are beyond the scope of this paper. But many others have been thinking about them, especially with regard to chemical and biological weapons. Gary Hart, for one, co-chair of the commission charged with trying to define the future national security environment, writes:

U.S. intelligence will face more challenging adversaries in the future, and nonstate actors will probably play a larger role in issues of war and peace than they have heretofore.<sup>65</sup>

As Gideon Rose observes:

The intelligence community is now challenged, because the groups that cause the greatest concern—religious fanatics, cults, and freelance extremists—are precisely those that

usually fly below the radar screen of standard intelligence collection.<sup>66</sup>

Collecting intelligence on biological weapons programs—even state-run programs—is especially difficult. For example, the IC did not know of Aum Shinrikyo's efforts to produce and use biological agents until after the sarin attacks in the Tokyo subway.<sup>67</sup>

That attack illustrates several problems that chemical and biological weapons present for the IC. Not enough attention is paid to open-source material; international cooperation is lacking; and there is not enough information-sharing even among U.S. IC organizations.

Nearly a year before its attack on the Tokyo subway system the Aum Shinrikyo group had used the nerve gas sarin in assaults on civilians. Although the Japanese media had reported the news, the U.S. government remained in the dark. Not only did Washington not hear what the Japanese law-enforcement agencies knew, but the Japanese agencies themselves were not aware of what other local organizations in Japan had uncovered. The parties involved did not share their expertise to prevent another attack.<sup>68</sup>

To this day, as Ashton Carter, John Deutch, and Philip Zelikow argue, the U.S. IC lacks a site and a methodology for conducting comprehensive planning of information collection. These experts contend that yields from such sources as overhead reconnaissance, electronic surveillance, clandestine agents, law enforcement databases and informants, and reports from foreign governments can be sifted and organized for maximum effect.<sup>69</sup>

Open-source collection, or lack of it, concerns Morton Halperin, who believes that most of the information today's security policymakers need is available without cloak-and-dagger work. "It is available from open sources, it is available from experts who know the societies, and it is available by going to the countries and dealing with the people."<sup>70</sup> U.S. policymakers now rely primarily for their

information on an IC in thrall to the notion that the best way to obtain information is to gather it secretly, from an unwitting source.<sup>71</sup> But instead of focusing on recruiting agents in foreign governments and intercepting messages from satellites, perhaps paying attention to the open press, as the IC should have been doing in Japan before the Tokyo subway attack, would be less costly and more productive.

Although neither Halperin, Carter, Deutch, nor Zelikow directly address creating a new IC, they do suggest some changes to the current structure. Halperin believes that a new research organization, called the Foreign Policy Research Organization or the Central Research Organization, should be created and moved out of CIA headquarters to downtown Washington. It should be housed in a building with easy access and staffed with analysts who understand that for most subjects that policymakers care about—not all, obviously, since there will always be some for which more traditional methods of collection are appropriate—most relevant information can be gathered from public sources.<sup>72</sup> Carter, Deutch, and Zelikow believe that a new institution to gather intelligence on catastrophic terrorism (which includes chemical and biological terrorism) needs to be established. It would be called the National Terrorism Intelligence Center and would collect and analyze information in an effort to provide advance warning catastrophic events. Their Center would be located at the FBI instead of the CIA and would have access to domestic law enforcement data.

The director of the center would come alternately from the FBI and the CIA, and all intelligence organizations would provide a specified number of professionals.<sup>73</sup>

Richard Falkenrath agrees that changes are needed in the IC to address the threat of chemical/biological terrorism, but his suggestions are functional rather than structural.<sup>74</sup> He feels it is important that the IC watch for the likely signatures of small-scale, improvised chemical and biological weapons programs both in the United States and

abroad. He also emphasizes that public health capabilities need to be improved—particularly epidemiological surveillance—in order to detect medical evidence of chemical and biological weapons production or use.<sup>75</sup>

All these recommendations are important. Intelligence is the first and most crucial line of defense against chemical and biological weapons attacks.<sup>76</sup> Chemical and biological warfare (CBW)-related intelligence is unusually difficult but not impossible. Would-be terrorists have problems as well as advantages; and conspiracies are relatively easy to defeat if law enforcement authorities learn of their existence with adequate lead time and in sufficient detail.<sup>77</sup>

### Who's in Charge? Who Should Be?

*Domestic Threats.* Critics argue that current U.S. efforts to prevent or respond to biological and chemical terrorism are spread across a vast number of agencies, at different levels of government, with little real coordination or direction. "Bureaucratic styles and missions clash; information is compartmentalized and left unanalyzed; some tasks are duplicated, while others slip through the cracks."<sup>78</sup> This is especially true of domestic incidents. Detection capabilities are limited; integrated analytical and planning efforts are proclaimed but not fully worked out; and the use of military forces—the most capable of dealing with biological and chemical weapons—is limited by the Posse Comitatus laws. It is by no means clear how all the moving parts of a response to such an attack within the United States would actually function in relation to one another.<sup>79</sup>

Although not a response to a biological weapons attack, the reaction to the recent outbreak of a mosquito-borne virus in New York is instructive. New York City and parts of the state suffered an outbreak of what appeared to be an encephalitis virus. What was initially identified as St. Louis encephalitis—often found in the southern United States—turned out to be West Nile virus. Fortunately, West

Nile virus is less virulent than the St. Louis variety; but the initial failure to identify the virus correctly has many concerned. "The encephalitis outbreak in New York is a powerful lesson for public health authorities," remarks Alan Zelicoff, a senior scientist at the Center for National Security and Arms Control at Sandia National Laboratories in New Mexico. "It is a sobering . . . demonstration of the inadequacies of the U.S. detection network for emerging diseases, including viruses."<sup>80</sup> A fact not lost on local and federal officials responsible for national defense against biological warfare is that the myriad local, state, and federal agencies involved in the New York encephalitis investigation did not always communicate well.<sup>81</sup> Initial samples from victims were screened only against six viruses common in the United States, and investigators did not test for viruses that have been linked to germ warfare.<sup>82</sup> We may never know how a West Nile-like virus suddenly appeared in New York City. But we do know that the United States has far to go before it is prepared to identify and deal with outbreaks of exotic diseases, whether they are spread by nature or deliberately by man.

Presidential Decision Directive (PDD) 39 decrees how the United States should be organized to deal with the use of WMD by terrorists. PDD 39 divides the threat, both at home and abroad, into two categories: crisis response and consequence management.<sup>83</sup> "Crisis response refers to instances where the perpetrators of an assault have been discovered before an actual release."<sup>84</sup> Consequence management refers to ways and means of reducing the short-term and long-term effects of an attack.

Domestically, the Department of Justice is the lead agency, with the Federal Bureau of Investigation (FBI) responsible for crisis management and FEMA for consequence management. Although DoD has the largest capability for chemical and biological defense, the main responsibility for dealing with attacks falls on multiple federal, state, and municipal agencies and on the civilian health community. "Most of these organizations are

inadequately prepared to deal effectively with the problem.”<sup>85</sup>

The assignment of domestic responsibilities under PDD 39 is a matter of debate among policymakers and academics, in two respects. First, there is disagreement about the separation of crisis and consequence management. Next, there is disagreement about who should be in charge.

Although PDD 39 has been an important catalyst for developing anti-CBW strategies, the categorical distinction it draws between preventing and dealing with the consequences of an attack is dangerously flawed.<sup>86</sup> Chris Seiple writes,

Given the varied dimensions and manifestations of chemical and biological terrorism, the battle of consequence management has been lost if there has not been consultation and planning well before any threat of an incident emerges.<sup>87</sup>

We must therefore think of crisis response and consequence management as parallel and overlapping continuums that both federal lead agencies and the first responder must keep constantly in view. . . . Arbitrary distinctions between activities before and after an attack by WMD cannot be extended into planning and operational activities. Should we allow those two continuous and overlapping processes to be compartmentalized—and thus expressed in a simple linear logic because they are considered mutually exclusive—we will fail in our response and thus invite future attacks.<sup>88</sup>

PDD 39 notwithstanding, there is no fine line during or after an attack that allows for a clean transfer of responsibility between the FBI and FEMA.<sup>89</sup> Almost inevitably there will be a “who’s in charge” or unity-of-effort problem. This structural confusion is compounded by the FBI’s overriding commitment to collecting criminal evidence. The FBI’s philosophy is: if you can’t prove who did it, the likelihood of future incidents will increase.<sup>90</sup> This is a useful approach to bank robbery or kidnapping, but not necessarily to chemical or biological weapons. The effectiveness of consequence management depends on the



quick collection of samples to determine the nature of the agent used and the level of contamination. Solving a crime also depends on collecting samples, but for evidentiary purposes. There is thus, at least in theory, a potential conflict between casualty reduction and criminal investigation.<sup>91</sup> In practice, in order to ensure that there is one overall Lead Federal Agency (LFA), PDD 39 directs FEMA to support the Department Justice (i.e., the FBI) until the Attorney General transfers the overall LFA role to FEMA.<sup>92</sup>

Presently, FEMA is the right agency for consequence management. Many of the coordination-and-control procedures that FEMA has developed over the years in the course of disaster relief efforts are appropriate for its WMD role. The same cannot be said for the FBI. As many experts have pointed out, biological and chemical weapons are simply not a specialty of the FBI. And where the potential for catastrophic terrorism is concerned, the FBI's reactive law enforcement approach needs to be supplemented by—perhaps even subordinated to—a more aggressive national security effort directed by the White House and the Pentagon.<sup>93</sup> Carter, Deutch, and Zelikow propose that if a large-scale biological or chemical attack is imminent, the PDD 39 structure should be pushed aside. They believe that the White House should immediately take charge. Unity of command would be vital, with an operational command structure able to “direct everything from CIA covert operations to air strikes; set up interdiction on ground, at sea, and in air; mobilize thousands of soldiers; and move thousands of tons of freight.”<sup>94</sup>

None of these actions can happen quickly unless plans have already been drawn up and units designated to carry them out, with repeated training and exercises that create the readiness to bring the plans to life. In this situation, the Defense Department would take the leading role. The FBI neither commands the resources nor plans to command them.<sup>95</sup>

In my opinion, Carter and his colleagues are correct. Because it has long prepared to face the grim possibility of chemical and biological weapons on the battlefield, and because it has experience in commanding and controlling large, multifaceted operations, the military has unique capabilities to offer in the domestic-security arena.<sup>96</sup> Currently, participation by DoD and the U.S. military as lead agencies in a domestic attack is problematic. For one thing, there are legal constraints preventing DoD from taking such a role. For another, DoD does not want the job.

The American military is constrained in conducting domestic military operations by the Posse Comitatus Act, which prohibits the Army and Air Force from enforcing civil or criminal law within the United States.<sup>97</sup>

This historic law, passed in 1878 to preclude the presence of soldiers from deterring voters during Reconstruction, is generally considered a great bulwark in our democratic society. Its proponents cite Posse Comitatus as a clear demonstrable indicator of the properly circumscribed limits of a civilian-controlled army in a representative democracy.<sup>98</sup>

In discrete instances, when the President of the United States believes public order and domestic tranquility are at risk, he can order the Secretary of Defense to restore public order. "This presidential authority to use federal troops is plenary and not subject to judicial review."<sup>99</sup>

Even though the President has the authority to use federal troops under certain circumstances, instances of such use have been rare. Posse Comitatus remains a "giant bulwark" against DoD participation in domestic operations. This is well understood in the Pentagon, as Secretary Cohen has made clear:

As in the past, any military support [in the wake of a domestic attack] must be just that—support. Both legal and practical considerations demand it. The Posse Comitatus Act and the Defense Department's implementing policies are clear—the military is not to conduct domestic law enforcement without

explicit statutory authority, and we strongly believe no changes should be made to Posse Comitatus.<sup>100</sup>

DoD has repeatedly affirmed that all military assistance for either crisis response or consequence management will be in support of the Department of Justice (FBI) or FEMA.<sup>101</sup> DoD has recently established a Joint Task Force-Civil Support (JTF-CS) to coordinate military support to the lead agencies and to other state and local authorities.<sup>102</sup> The emphasis is on support, and there are no plans for the JTF-CS to take a leadership role in crisis management or response. Its mission is to support designated LFAs with a standing joint organization providing DoD's consequence management capability in response to domestic biological and chemical incidents.<sup>103</sup> According to some reports, however, differences have surfaced over which agency is best prepared for rapid response.

Less than a year after the U.S. Department of Defense created rapid response units to respond to WMD attacks in the U.S., their role has become the subject of debate between federal agencies. DoD officials, backed by the Clinton administration and Congress, insist that only specialized military teams have the training and resources to adequately respond to a catastrophic . . . biological or chemical attack in the U.S.<sup>104</sup>

DoD contends that specially trained Army National Guard Rapid Assessment and Initial Detection (RAID) teams and the Marine Chemical/Biological Response Force (CBIRF) are best prepared to respond to large-scale disasters, and it has recently expanded the number of RAID teams. On May 22, 1998, Secretary Cohen announced the initial plan: 10 regional RAID teams composed of 22 highly skilled full-time National Guard personnel.<sup>105</sup> On June 2, 1999, the Clinton administration requested 5 more teams, and the Senate Armed Services Committee has requested an additional 17, so that as many as 27 RAID units could be dispersed throughout the country.<sup>106</sup>

FEMA and FBI officials contend that the more than 600 hazardous material (HAZMAT) organizations throughout the nation could handle detection and decontamination better than their RAID counterparts. Since there are more of them, it is argued, they could usually respond quicker, and they have more experience cleaning up hazardous material. DoD and congressional officials counter that civilian HAZMAT squads usually respond to industrial accidents and have little, if any, experience with the chemical and biological agents that RAID teams are trained to deal with.<sup>107</sup>

GAO agrees with the FBI and FEMA, and in a recent report asked Congress to consider abolishing the RAID units. According to the GAO, because RAID teams do not have dedicated airlift, they probably could not get to the site fast enough to help local responders.<sup>108</sup> In a chemical incident, for example, the first hour or two are critical, but RAID teams cannot guarantee a response time of less than 4 hours.<sup>109</sup> In the event of a biological weapons attack, the usefulness of the RAID teams is even more questionable, critics say.

Because germ agents such as anthrax or smallpox can be released inconspicuously, there is little likelihood of knowing an attack has occurred until hours or even days later, when sick people start showing up at hospitals or doctors' offices.<sup>110</sup>

Pentagon officials call the teams the "tip of the military spear" that would help civilian agencies tap into other military assets.

The idea is that the RAID teams would help local and state first responders—primarily firefighters, HAZMAT teams and ambulance crews—identify chemical or biological substances used in a terrorist incident and then, if necessary, plug them into the military's pool of weapons and logistics experts.<sup>111</sup>

The GAO replies that state and local officials do not agree that RAID teams are needed but instead believe they represent "an unnecessary duplication of assets."<sup>112</sup>

Officials from larger jurisdictions usually have very robust HAZMAT capabilities. These officials consider themselves very experienced in managing HAZMAT emergencies and did not believe the RAID team could suggest anything they did not already practice every day.<sup>113</sup>

Taking sides in this GAO-Pentagon debate is not the purpose of this chapter. It is, however, worth noting that the debate indicates the problems associated with the

mind-numbing array of government agencies—sixty-one in the federal government alone, according to the Center for Nonproliferation Studies—that play some kind of role in domestic defense.<sup>114</sup>

Add to these the hundreds of state, county, and municipal public safety organizations throughout the United States that could claim some type of jurisdiction in the event of a terrorist attack, and the extreme complexity of response coordination becomes obvious.

Other nations faced with similar threats have more streamlined response mechanisms. A look at how three of them—Israel, the United Kingdom, and Canada—are organized to address chemical and biological terrorism may be useful.

### The Israeli Model.

Many Middle Eastern countries are now capable of delivering chemical and biological weapons. Operation DESERT STORM demonstrated the threat to Israel in this regard. In 1992, under the leadership of Major General Zeev Livne, the Home Front Command was established with three major responsibilities: to prepare civil defense forces for emergencies; to create a central command for all military and emergency forces; and to serve as the primary military and professional authority for civil defense.<sup>115</sup>

Along with overseeing civil defense, rescue and salvage, and domestic security, the Home Front Command also helps

civilian authorities maintain equipment and protective gear at service centers throughout the country, staffs an around-the-clock information center to answer civilian queries, and is responsible for developing means of passive protection. For example, in cooperation with the United States, the Command conducts demolition tests to determine the ability of certain materials and structures to withstand attack. All new homes in Israel must now have a "safety zone" that can withstand all but a direct hit from a missile.<sup>116</sup>

To assist the population in preparing for emergencies, an instructional and information division serves in peacetime as well as wartime. Schools and other institutions receive training from special instructors. The Home Front Command has installed some of the world's most advanced control, communication, and electronic warning systems throughout Israel, monitored by a national control center capable of broadcasting real-time messages to the entire population. The Command's forces are of four kinds: rescue and salvage troops, medical support personnel, fire-fighting personnel, and anti-nuclear, biological, and chemical (NBC) units. Rescue and salvage units are the Command's primary forces, employing a wide range of equipment to locate victims and deal with casualties. A national rescue and salvage unit is on constant alert for both domestic and international rescue missions, and some of these units have recently served with distinction in Turkey and Greece.<sup>117</sup>

In an emergency, the Home Front Command can merge military and civilian fire-fighting and medical units. Medical services, including ambulances, medical corps personnel, and hospitals, hold frequent exercises. Anti-NBC units, including detection and identification teams, are prepared to handle all aspects of response, from identifying substances to decontaminating affected areas. The National Hazardous Materials Information Center operates within the Home Front Command in cooperation with the Ministry of the Environment, providing updated information and online risk assessment for troops in the

field. The Center operates around the clock, in peacetime as well as wartime.<sup>118</sup>

Military guards, drawn partly from the army's combat units, are another level in the Command's hierarchy. They are constantly engaged in maintaining security along Israel's border and shoreline and in protecting vital infrastructure. Ninety-seven percent of those serving in the Home Front Command are in the reserve forces. Nevertheless, the Command has equal stature with the three other Front Commands, which are made up of active and reserve forces and have border area responsibilities.<sup>119</sup>

Israel's volatile geopolitical situation—along with the advances in missile technology available to its neighbors—has rendered the country exceptionally vulnerable and necessitates a nontraditional organization like the Home Front Command. During the state of alert in December 1998, the Command established 67 gas mask distribution centers throughout the country, which remained open 24 hours a day and could even have supplied tourists if necessary. Hospitals were prepared to deal with chemical and biological casualties. Decontamination stations were equipped and staffed.<sup>120</sup> A robust exercise program, not limited to military and public-safety organizations, helps the society prepare for contingencies: for example, an exercise last April named "Netanya '99" put one of Netanya's high schools through a drill mimicking the effects of a chemical attack.<sup>121</sup>

The Home Front Command is in charge of civilian forces in peace and war. This differs from the practice of most other democracies and, according to General Livne, was initially "a very difficult concept for civilians to accept." But Israelis understand unity of command—an unequivocal and unambiguous chain of responsibility, authority and accountability<sup>122</sup>—and so eventually the public has accepted military control via the Home Front Command as the most logical way to prepare for attacks with WMD.<sup>123</sup>

The old military maxim that the best defense is a good offense is official Israeli policy. The Israelis will take preemptive action if policymakers have good intelligence and there is a reasonable chance of success. In 1981 Israel had intelligence that the Osirak nuclear reactor in Iraq would produce weapons-grade fuel as a by-product. On June 7, 1981, Israeli Air Force pilots flying F-16s bombed the Osirak facility.<sup>124</sup>

The raid was skillfully planned. When the Israeli pilots were in Jordanian airspace they conversed in Saudi-accented Arabic and informed Jordanian air controllers that they were a Saudi patrol gone astray: over Saudi Arabia they pretended to be Jordanians. The first wave of F-16s punched a hole in the reactor dome, after which a second wave of aircraft dropped "dumb" (that is, not laser-guided) bombs with enough accuracy to destroy the reactor core, its containing walls, and the gantry crane.<sup>125</sup>

The Israelis also use retribution to deter terrorism. Following the 1972 massacre of Israeli athletes at the Munich Olympics and a wave of attacks on Israeli diplomats and other civilian targets, Prime Minister Golda Meir decided on a new tactic.<sup>126</sup> The enemy in this case was the shadowy Palestinian group "Black September," established by Yasir Arafat to carry out nonattributable terrorist attacks while the political wing of the PLO moved toward international respectability.<sup>127</sup> The Israeli answer to Black September was a group called "Wrath of God." In the months following Munich, Wrath of God relentlessly struck back at Black September, conducting daring raids into Beirut to kill the top leadership and tracking down and assassinating other operatives in Europe and elsewhere. By late 1973 Black September had effectively ceased to exist, its few remaining members demoralized and fearful.<sup>128</sup> Although the activities of Wrath of God did not end Palestinian terrorism, it disrupted its operations and undermined its capabilities.<sup>129</sup>



## The United Kingdom Model.

Because the United Kingdom (UK) is a unitary state and a parliamentary democracy, it has advantages over the United States in preparing for and responding to chemical or biological attacks. In contrast to federal systems like the United States and Canada, where power is shared between the central government and state or regional governments, in Britain no powers are reserved for sub-national units of government. The UK does not have several layers of public security organizations as in the United States, where federal, state, county, and city police agencies co-exist. Instead the UK has 43 police constabularies. Each constabulary is independent and is commanded by a Chief Constable.<sup>130</sup> Major public-safety actions of a multi-constabulary or national character are coordinated through the National Reporting Center at Scotland Yard (London Police Headquarters) and the Home Office.<sup>131</sup> Questions of jurisdiction do not arise. After the Oklahoma City bombing, 26 federal, state, county, and city agencies could have plausibly claimed jurisdiction over one or another aspect of the investigation.<sup>132</sup> Had a similar tragedy occurred in the UK—say in York—the Chief Constable responsible for York would have been in charge. No one else. Fire-safety forces are organized similarly within the 43 constabularies, which improves response time, operational efficiency, and coordination.<sup>133</sup>

The UK's parliamentary system functions more expeditiously in some respects than presidential systems because Parliament combines executive and legislative functions. It can make or overturn laws and establish policies without recourse by the executive, the judiciary, or the monarch. In the United States, executive policy is subject to checks and balances by the legislature and judiciary. In the UK, once policy is set by Parliament, only Parliament can change it.<sup>134</sup> This fusion of legislative and executive powers is expressed in the cabinet.<sup>135</sup>

Through its collective decision making, the cabinet . . . shapes, directs, and takes *collective responsibility* for government. Cabinet government stands in stark contrast to presidential government and is perhaps the most unique feature—and certainly the pivot—of Britain's whole system of government. For it is the body, where the executive and legislature overlap, that control of government rests.<sup>136</sup>

The Home Office, headed by the Home Secretary, is responsible for internal affairs. In the event of a biological or chemical attack in the UK, crisis and consequence management would be the responsibility of the Home Office. The Home Secretary, his deputy, or another representative would chair an interdepartmental cabinet-working group assembled to manage the event. At a minimum, the Ministry of Defense, Special Branch (MI 5), the Secret Intelligence Service (MI 6), and the Foreign Office would be represented.

At the tactical level, the Chief Constable of the affected region is in charge of ground operations. The Ministry of Defense plays an advisory role unless police forces cannot accomplish their mission. If Defense takes charge of the operation, a written document establishing responsibility and accountability is passed from the Constable to the on-site military commander. When the situation is again within the capabilities of the police, the document is passed back and the military returns to an advisory capacity. For example, during Operation Nimrod, the 1980 British Special Air Service (SAS) raid to retake the Iranian Embassy in London from terrorists, responsibility did not transfer to the SAS military unit until the final hour of the operation. The crisis began at 11:32 a.m. on April 30. The SAS did not receive operational control until May 5 at 7:07 p.m., when

the senior policeman on the scene handed Mike Rose, the commander of 22nd SAS, a signed piece of paper which effectively handed control of the situation over to the SAS.<sup>137</sup>

By 7:40 p.m. the SAS had retaken the embassy and “quickly disappeared from the scene before the press showed up.”<sup>138</sup>

An SAS team is stationed permanently in London and is responsible to Scotland Yard and ultimately the Home Secretary. The SAS operates under strict guidelines within the UK, and team members, aware that they are liable to prosecution if they employ excessive force, walk a fine line. To repeat: for the SAS to be used, the operation must be beyond the capabilities of civilian police, and written authority must pass from civilian authorities to the military.<sup>139</sup>

Three threat levels—gold, silver, and bronze—determine the nature of the response and the membership of the interdepartmental cabinet-working group. A “gold” event would be classified as catastrophic in the United States and would entail maximum availability of resources. The Prime Minister would be closely involved, perhaps even chairing the working group instead of the Home Secretary. If foreign involvement were found, the Foreign Minister and Defense Minister would probably have responsibility for out-of-country negotiations and operations.

“Silver” is a serious domestic event with no apparent international involvement. The cabinet working group would be manned at the Minister or Deputy Minister level, and the military would probably remain in an advisory role. A “bronze” event is one that can be handled at the local constabulary level.<sup>140</sup> Frequent exercises are held at all three levels to allow potential members of the interdepartmental working groups a chance to work together.

As a unitary state with a parliamentary democracy, the UK has some advantages over the United States in handling domestic terrorism. It also has considerable experience: having conducted a counter-terror campaign in Northern Ireland for more than two decades, UK security forces have learned much.<sup>141</sup>

## The Canadian Model.

Throughout its history, Canada has relied on its military to put down rebellions, ethnic confrontations, election violence, strikes, prison violence, and terrorism.<sup>142</sup> Domestic use of Canada's armed forces continues today.

In the past two years large portions of the Canadian Forces have been involved in support of the civilian authorities. This support has included humanitarian assistance to fight floods, forest fires and ice storms.

In the case of the Red River flood of 1997 and the severe ice storm of 1998, the military provided assistance to law enforcement agencies as well as ordinary humanitarian support.<sup>143</sup> The Canadian Forces are often asked to supplement civilian security forces at important domestic events, like the 1976 Montreal Olympics, visits by foreign dignitaries, and the G7 Summits in Montebello and Halifax.<sup>144</sup> Among other duties at such events, the Canadian Forces maintain specially trained rapid-response counterterrorism and bomb-disposal units.<sup>145</sup>

The Canadian military can perform this role because Canadian law allows the timely use of military forces in domestic emergencies. In 1988 the Canadian government restructured and simplified its laws in this area. The Emergencies Act identified four types of emergencies: "public welfare (severe natural disasters); public order (threats to the internal security of Canada); international; and war."<sup>146</sup> The Act specifies the powers the government is allowed in each kind of situation. In a Public Order Emergency, for example, the government is

authorized to prohibit public assembly and travel to and from a specified area, and to designate and secure protected places, assume control of public utilities, and impose summary convictions for up to six months of imprisonment.<sup>147</sup>

The new act also addresses threats posed by Canadian groups receiving outside support; officials "would have the

option of declaring either a Public Order Emergency or an International Emergency in such a situation."<sup>148</sup>

Companion legislation, called the Emergency Preparedness Act, established an organization known as Emergency Preparedness Canada (EPC) under the jurisdiction of the Department of National Defense. Pursuant to this act,

federal and provincial government departments must create administrative machinery and cooperative contingency plans at the provincial level with the Department of National Defense and Emergency Preparedness Canada to respond to the four types of emergencies described in the Emergencies Act.<sup>149</sup>

In times of civil unrest or national crisis, provincial premiers and the Solicitor General may ask the military to act in support of police and civil authorities. The Canadian military has provided crowd-control, policing, counter-terrorist, and other forms of support, withdrawing as soon as civil authorities are able to resume control.<sup>150</sup>

A 1994 Defense White Paper, reflecting the end of the Cold War, further refined the domestic roles and missions of the Canadian military. The White Paper specified seven areas in which forces of the Department of National Defense could be deployed: peacetime surveillance and control (sovereignty protection); securing Canadian borders against illegal activity (counter-narcotics); fisheries protection; environmental surveillance; disaster relief; search-and-rescue; and counterterrorism.<sup>151</sup> It also directed that the national dynamic entry (counterterror-hostage rescue) mission be transferred from the Royal Canadian Mounted Police Special Emergency Response team to the army's JTF-2 counterterror unit.<sup>152</sup>

The Canadian approach to supporting civilian authority is extremely flexible. It relies on a carefully designed legal framework and a professional force structure.

Legislation does not prescribe the exact civil-military relationship at the operational and tactical levels, nor does it hamper commanders by dictating the levels of response which may be required in violent situations.<sup>153</sup>

In general, Canadian law avoids overly explicit restrictions on the military.<sup>154</sup> This flexibility points up significant differences between Canadian and American political and legal cultures. The Canadian government places great confidence in military professionalism, doctrine, and training. In the United States, on the other hand, the Posse Comitatus Act limits the involvement of the armed forces much more sharply and places severe restrictions on the scope of their activities, even when the military is clearly more qualified than its civilian counterparts to undertake the mission in question.

### Organizing for Success.

This brief review of how Israel, the UK, and Canada organize themselves against domestic threats, including those posed by biological and chemical weapons, prompts several observations. First, all three democracies have specified procedures for the use of active and reserve military forces in domestic security matters. In Israel the military is the lead agency in countering domestic threats, and its Home Front Army actually has authority over some civilian agencies in both war and peace. In the UK, and to a somewhat lesser extent in Canada, the military normally plays a supporting role, though when circumstances dictate, it can become the lead agency in a domestic crisis. In the UK, transfer of authority to and from the military is accomplished by a written document, much like a contract, and the duration of military control is typically very short. In Canada, the time frame for transition to and from military control is established by the laws and policies described above.

As noted, all three states have parliamentary systems, which make for more streamlined policymaking than our

presidential system. Israel and the UK are unitary states, not hampered by several layers of jurisdiction. Canada, though a federal system, mandates that federal and provincial departments create common plans and administrative procedures for responding to several types of emergencies, including CBW attacks.

The United States can learn much from these three allies. All three, though robust democracies, understand that unity of command is essential for proper response to a catastrophic event and that military organizations are more suited to dealing with some types of domestic threats than are civilian organizations. This is particularly true of CBW threats, because combat troops are trained to survive on a contaminated battlefield. Such training is indispensable in an age in which rogue states, failed and failing states, and nonstate actors, lacking the means to confront advanced militaries in conventional conflict, may well choose CBW in order to offset this inferiority.<sup>155</sup> Israel, the UK, and Canada understand that military organizations intensively plan, organize, equip, and train for complex emergencies and that military commanders understand how to organize and coordinate multiple organizations for a common objective. Why not, they might ask their U.S. counterparts, make use of these distinctive capabilities in domestic emergencies?

There may also be other lessons here. Israel's use of preemption and retribution is instructive. During the Cold War, the United States successfully relied on nuclear deterrence to prevent an attack on its homeland. Preemption and retribution were not plausible options in the highly charged nuclear environment. Some commentators, like columnist John Ellis of the *Boston Globe*, believe that nuclear deterrence is still an option. The United States must "develop a plan for massive retaliation in the event of a biowarfare outbreak." That plan should be made public, Ellis writes, and broadcast around the world. "One way for biological agents to 'blow back' on those who launch them is nuclear retaliation."<sup>156</sup> It makes sense, argues Jessica Stern, "for governments to signal their

intention to respond to state-sponsored terrorist acts with massive retaliation that may even include the use of nuclear weapons.”<sup>157</sup> Others question the practicality of nuclear deterrence in a threat environment populated in large part by nonstate actors. Threatening to retaliate with nuclear weapons for acts of chemical or biological warfare would not be proportional, they contend, and might undermine efforts toward nuclear nonproliferation.<sup>158</sup> Moreover, the Tokyo subway and Oklahoma City attacks were perpetrated by local residents. How could we have deterred them with nuclear weapons?

Israel’s successful record of preempting terrorist attacks is based on good intelligence and an ability to infiltrate terrorist organizations. The United States has lagged in this regard, as illustrated most recently by the targeting of a suspected chemical weapons plant in Sudan in an attempt to preempt Osama bin Laden. Unfortunately, it now appears doubtful that there was a clear link between the Al Shifa plant in Khartoum and Mr. bin Laden, or that the plant was making chemical weapons.<sup>159</sup> Interestingly, however, Washington’s mistake may still have had the desired effect.

Sudan, which has tried for months to convince Washington that it does not support international terrorism, advised the United States on May 22, 1999, that it will sign several anti-terrorism accords and the 1993 convention banning chemical warfare.<sup>160</sup>

Could it be that the continued threat of preventive military action, even if misplaced in this instance, convinced the Sudanese to change their behavior?

The dangers of CBW proliferation and use by terrorists warrant the consideration of special preventive measures. The political risks and operational difficulties are substantial but not prohibitive and may well be outweighed by the benefits. Once a CBW program has been underway for some time, the operational requirements for a successful preemption—from accurate intelligence on facilities and



sites to target destruction without unacceptable collateral damage—are likely to be very high,<sup>161</sup> although the political risk will be lower to the extent there is evidence of the adversary's capability and intent. From a military perspective, however, the time to strike is at an early stage, when the operational requirements are more manageable but the political risks are greater.<sup>162</sup> Israel often opts, after a cost-benefit analysis, for early action. The United States should consider the early option too—though only when it has developed a better intelligence capability.

As mentioned earlier, the Israelis are meeting the threat of chemical and biological terrorism with a Home Front Command, 97 percent of whose members are reservists. This notion has advocates in the United States. Deborah Lee, Assistant Secretary of Defense for Reserve Affairs, has observed:

The U.S. military reserve components are the appropriate forces to use in homeland defense and WMD response. They live and work in all communities and they have established links to the fire, police and emergency medical personnel who are always the first to arrive at the scene of any incident. Consequently, the Guard and Reserves represent a unique pool of manpower and expertise that, with the proper training and equipment, can support local, state and federal authorities.<sup>163</sup>

The Reserve and Guard bring different advantages to domestic CBW response. Most of the chemical and medical units are located in the Army Reserve.<sup>164</sup> Those in the Guard are largely at the division level and are dedicated to units programmed for international deployments and other contingencies.<sup>165</sup> The Guard's advantage is that, unless federalized, it is an instrument of the governor of the state and not covered by the Posse Comitatus Act. It may therefore enforce civil laws. Once federalized, the National Guard, like the Active Army and the Army Reserve, comes under the Posse Comitatus Act and no longer may be used to reinforce local law enforcement agencies.<sup>166</sup>

The UK model offers American policymakers some interesting organizational insights. The interdepartmental working group process within the UK cabinet is more responsive and less cumbersome than the current interagency process in the United States. In the UK, the Home Secretary is in charge and the others at the cabinet table are from the Foreign Office, the Ministry of Defense, the Police and Intelligence Services, and other ministries as necessary. They plan and exercise together and with the 43 police constabularies throughout the nation. During an emergency, and depending on the level and type of crisis, the Home Secretary assembles the participants and the Home Office manages the response.<sup>167</sup>

By comparison, the Senior Interagency Coordination Group (SICG) charged with identifying, discussing, and resolving issues regarding the federal response to CBW incidents, is composed of six senior members (from FEMA, FBI, DOE, EPA, the Department of Health and Human Services (DHHS) and DoD, as well as representatives from the Department of Agriculture, the Department of Transportation, the Bureau of Justice Assistance, the U.S. General Services Administration (GSA), and the National Communications System.<sup>168</sup> The SICG is a coordinating organization, does not exercise, and has no operational responsibilities; nor does it coordinate the myriad state, county, and city agencies involved in CBW response.

Another aspect of the British system that may be transferable is the “gold, silver, bronze” level of threat assessment and response. In that system, the level of mobilization and the rank of those involved corresponds to the level of threat. Gold, silver, and bronze responders know who they are and plan, train, and exercise together. Carter, Deutch, and Zelikow are among those who have recognized the utility of identifying different threat levels.

The United States needs a two-tier response structure: one for ordinary terrorist incidents that federal law enforcement can manage with interagency help, and another for truly

catastrophic terrorist attacks. The government would require two new offices, one within the office of the defense secretary, and the other within the existing [Joint Forces Command] which already bears operational responsibility for the defense of the American homeland and the majority of U.S. armed forces. These Catastrophic Terrorism Response Offices (CTROS) would coordinate federal, state, and local authorities as well as the private sector to respond to major terrorist threats once they are activated by the president and the defense secretary.<sup>169</sup>

One aspect of the Canadian model may be readily applicable in the United States. The close contingency-planning relationship between Emergency Preparedness Canada and the Department of National Defense could and should have an American counterpart other than the currently overburdened and often criticized FEMA.<sup>170</sup> The EMC-DND relationship, as the reader may recall, is part of the Emergency Preparedness Act, which stipulates how provincial and federal organizations are to coordinate emergencies.<sup>171</sup>

### Recommendations—Domestic Threat.

From the preceding survey of potential threats and other states' preparations for them, a number of recommendations emerge. Chief among them: change the National Security Act to reflect security requirements in the post-Cold War world. Include in the Act the legal framework and the organizational and institutional structures necessary for homeland defense. Establish a civilian-led Homeland Defense Command that capitalizes on the strengths of the Reserve and National Guard, which are "particularly well-suited to an increased role in this area, as their infrastructure exists in all fifty states."<sup>172</sup> The participation of the Guard and the Reserve in disaster-relief operations has prepared them to undertake similar, though much more dangerous, counter-CBW operations. Whenever possible, use non-federalized National Guard units, which will not be hindered by Posse Comitatus restrictions. This is

especially important during crisis management, when support for law enforcement agencies is critical.

Some desirable measures may be more feasible than others. Establishing a Homeland Defense Command is unlikely, given the historical and cultural impediments to such an organization. But it should be possible to create a leadership structure embracing the FBI and FEMA which will insure that both crisis and consequence management are handled simultaneously, harmoniously, and efficiently.

FEMA is used to dealing with natural disasters and having to coordinate with local officials. But an act of terrorism would create both a crime scene and a disaster—making it necessary for agencies that do not usually work together to coordinate their efforts. “Oklahoma City was a good test case,” a FEMA official [said], “in the sense that it revealed the competing priorities of the FBI and FEMA. The FBI’s principal objective was to preserve evidence, while FEMA wanted only to save lives.”<sup>173</sup>

Moreover, FEMA is used to operating in an interagency and intergovernmental context, while the FBI is not. The FBI has traditionally been reluctant to assign its agents to interagency taskforces, much less lead them, because J. Edgar Hoover thought the FBI’s reputation might suffer if it had to share responsibility for mistakes caused by the bad judgment of other interagency members.<sup>174</sup>

John Deutch and the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (better known as the Deutch Panel) have called for a national coordinator with the rank of deputy assistant to the President with sufficient authority to “untangle the Gordian knot of jurisdictions that attempt to fight the spread of WMD and the means to deliver such weapons.”<sup>175</sup> In my view this recommendation, while a step in the right direction, does not go far enough. For one thing, the Deutch Panel did not address domestic response to acts of terrorism. For another, even with the rank of deputy assistant to the President, the

national coordinator they propose would be just that: an agency coordinator—convening meetings, leading the interagency policy process, allocating resources, making budget decisions, and reviewing technology-acquisition problems—rather than a leader with authority to direct agencies in times of crisis.<sup>176</sup> More appealing are the statements of Frank Cilluffo, director of the terrorism task force at the Center for Strategic and International Studies in Washington DC, who believes there should be a domestic terrorism “czar.” Testifying in October 1998 before a congressional subcommittee, Cilluffo argued for the creation of a new commander-in-chief to oversee homeland defense, under DoD. “What I’m saying is that you want one individual, you want it to be their single, primary mission.”<sup>177</sup>

If the Gordian knot is to be cut and the crisis management/consequence management dilemma resolved, one more coordinator, no matter what his or her rank or access, will not get the job done. What is needed is a national *director* with super-agency powers as well as ready access to the President and Congress. This official should be a deputy assistant to the President and reside at the National Security Council (NSC), which by its charter is responsible for advising the President on both domestic and international security. Currently the national coordinator for security, infrastructure protection, and counter-terrorism works at the NSC. Why not elevate this position to national director, with authority to direct agencies in the field? The Kissinger and Brzezinski periods, when the NSC was a “superdepartment” that provided guidance for both Defense and State, offers some idea of what the NSC with an operational mission might be like.<sup>178</sup>

The United States needs to enhance its biological and chemical warfare intelligence capabilities. If the IC did nothing else for the next 20 years but concentrate on biological weapons proliferation, writes John Ellis, “it would be money well spent.”<sup>179</sup> Most analysts do not go quite that far, but many argue that changes need to be made. As

Ernest May observes, what worked when the major threat came from communists in Moscow with nuclear weapons cannot be counted on to work when different enemies are wielding viruses and other WMD.<sup>180</sup>

It is also worth listening to those analysts and policymakers who believe that too much secrecy limits the effective use of intelligence, that too much emphasis is placed on collection and not enough on analysis, and that not enough use is made of open source material. At present admirals and generals routinely complain of not even knowing what they *can* be told.<sup>181</sup> How then can the ultimate consumers of domestic CBW intelligence—local law enforcement officials, doctors, or scientists not even in government employment (perhaps not even U.S. nationals)—hope to get timely information? They cannot; and thus effective classification, clearance, and dissemination are going to require new rules and perhaps new statutes.<sup>182</sup>

Jane Holl, principal editor of the Carnegie Corporation's *Preventing Deadly Conflicts*, estimates that 90 percent of the IC's budget goes to collection and 10 percent to analysis.<sup>183</sup> That ratio needs to be changed drastically. Raw intelligence is of little use to consumers; timely analysis is essential. It is all too possible at present that data pertaining to a CBW attack might get collected but not analyzed and disseminated to those who are charged with preventing an attack. I have already referred to the need to make better use of open sources. Had these been used, the Tokyo subway incident might have been prevented. Finally, one has to question the necessity for 13 separate intelligence agencies. Are that many really necessary? And if so, are they coordinated effectively? Probably not; consider that the Director of Central Intelligence—the head of the IC according to the National Security Act—only controls fifteen percent of the intelligence budget.

Much can be learned from America's major allies: Israel, the UK, and Canada. All are mature democracies, with their

militaries firmly under civilian control. Yet they have no Posse Comitatus restrictions and make effective use of military forces for homeland defense against many threats, including CBW and terrorism. Canada's Emergency Preparedness Act, which defines how its provincial and federal forces should cooperate during domestic emergencies, is worth emulating. So is the UK's streamlined interdepartmental cabinet decisionmaking process, with its multi-tiered response structure.

Israel's CBW threat-response organization and doctrine are particularly instructive. Though it is doubtful that Americans would agree to gas mask distribution offices in every population center—after all, many of our soldiers won't allow themselves to be vaccinated against anthrax—it is likely that they would agree with Israel's doctrine concerning preemption. Absent an effective deterrent, particularly against nonstate actors, the United States needs to think hard about the use of military force for preemption, which will be discussed in the following section of this paper.

Furthermore, it is time to review the Posse Comitatus Act. None of our allies imposes such strict prohibitions on its military. It no longer makes sense to prevent America's best-qualified CBW-response assets and counterterror forces, which happen to be in the military, from helping the nation cope with the CBW threat.

A final recommendation: put someone unambiguously in charge. As Israel's General Livne points out, the fight against terrorists armed with CBW is a war, and the first principle in war is unity of command. Achieve unity of command in addressing the domestic threat, and the rest will fall into place.

## International Threat.

The United States is in a much better posture to address chemical and biological threats internationally than it is

domestically. The Department of State is the lead agency for crisis response and consequence management overseas. State carries out crisis response through its Office of Counterterrorism, and consequence management through its Office of Foreign Disaster Assistance. The Department of Defense supports overseas counter-terror operations, including those against CBW. Walter Slocombe, Undersecretary of Defense for Policy, recently revealed that there are designated Special Mission Units (SMUs) manned, equipped and "trained to deal with a wide variety of transnational threats." According to *Jane's Defense Weekly*, the tactics, techniques, procedures, equipment and personnel of these SMUs remain classified, though it is understood that they have counter-terrorism and counter-proliferation responsibilities.<sup>184</sup>

Nevertheless, there are three areas that require urgent attention: force protection, lack of diplomacy, and doctrine. Our service personnel are the most vulnerable to chemical and biological attack, and our ability to protect them is not very good. In fact, the protective equipment the Army currently employs is little better than that employed when I was an infantry company commander 18 years ago.<sup>185</sup> As reported in the press, more than half the protective masks in the U.S. military have "critical" defects that might make them useless in protecting soldiers against gas or germ attacks, and many of the protective garments the Army purchased recently will not work.<sup>186</sup> In fact, over 10,000 masks, out of the 19,000 inspected, had at least one critical defect.<sup>187</sup> Also, 18,000 of the 880,000 "battledress overgarments" in Army stocks were found to be defective, while an additional 80,000 were labeled "suspect" and pulled for further testing.<sup>188</sup> The Air Force identified 45,723 "unserviceable" sets of BDOs in its supplies, about 5 percent of its total inventory. The Navy and Marine Corps did not have this problem: they have newer suits known as JSLISTs—Joint Services Lightweight Integrated Suit Technology suits. The Army is scheduled to begin issuing JSLISTs to some of its early-deploying units later this



year.<sup>189</sup> Clearly, the Army's priority should be to increase and accelerate procurement of these new suits, which permit much less degradation of operations under chemical and biological warfare attack than the older mission oriented protective posture (MOPP) suits.

This suit [i.e., the JSLIST] was designed to meet the needs of all military services. It has been designed to provide protection from the effects of nuclear, biological, and chemical (NBC) contaminants. It is lighter, less bulky, imposes less heat stress, and reduces physiological burdens compared to the service specific garments of the past. Attempts are now being made to improve the suit through the JSLIST P31 (Pre-Planned Product Improvement) Program. It is planned to leverage industry for mature fabric technologies for garment, glove, and sock designs and materials that provide improved chemical protection and fit, extend wear, and reduce bulkiness and heat stress. The current JSLIST garment design will be used, with minimum modification as required to obtain improvements.<sup>190</sup>

The goal should be to ensure that war fighters, who are put in harm's way, are equipped with the best protective gear that technology can provide.

U.S. inability to negotiate with rogue states and nonstate actors, and overreliance on treaties and conventions, limit the usefulness of diplomacy in reducing the likelihood of chemical and biological attack. For example, stated U.S. policy is not to negotiate with terrorists.<sup>191</sup> The rationale is clear: giving in to terrorist demands will prompt more terrorist activity. This is especially true in hostage-taking situations when negotiating involves the risk of having to meet terrorist demands for ransom or safe passage. However, it would be useful to have a mechanism—preferably secret—that enables regular dialogue with terrorists. This is especially important with transnational, nonstate actors, who have no formal diplomatic voice. The manner in which this dialogue takes place would vary. Discussions could be held in secret or through surrogates. Ideally, a dialogue could be established before an attack, with some hope of preventing

it. Dialogue is important if only because understanding what is really on a terrorist's mind has intelligence value. And letting a terrorist know our mind may well have deterrent value.

Nuclear arms control and reduction treaties promulgated during the Cold War were and still are valuable assets in preventing conflict. They provided baseline agreements that fostered cooperation and led to greater transparency and confidence-building measures that still exist today. Unfortunately, treaties meant to control and reduce the numbers of chemical and biological weapons have not been as effective.

The Chemical Weapons Convention (CWC) entered into force on April 29, 1997. It has been signed by 120 states and bans chemical weapons production and storage, as well as use. The strength of the convention is that it contains unprecedented and highly intrusive inspection provisions, including routine and challenge inspection mechanisms. The weakness of the convention is that several countries of chemical proliferation concern have not joined the CWC regime. These include Iraq, Libya, North Korea, and Syria.<sup>192</sup>

Biological weapons are also prohibited by a treaty—the Biological and Toxin Weapons Convention (BWC)—that entered into force in 1975 and now comprises some 140 members. The strength of the BWC is that it bans an entire class of weapons, prohibiting the development, production, stockpiling or acquisition of biological agents or toxins of any type or quantity that do not have protective, medical or other peaceful purposes. “The major shortfall of the BWC is its lack of any on-site verification mechanism.”<sup>193</sup>

Unfortunately, both the Chemical Warfare and Biological Warfare conventions affect only state behavior. They have no impact on the behavior of transnational and other nonstate actors who might possess and use CBW, nor on those rogues states that are not signatories to the conventions.

The major problem the United States has in addressing international chemical and biological threats is outdated military doctrine. The traditional uses of military force are defense, deterrence, compellence, and presence. Defense against biological and chemical attack, as mentioned earlier, is extremely difficult, especially in a democracy. Deterrence, especially against rogue and nongovernmental actors, is also difficult—where exactly do you strike Osama bin Laden if he launches a biological attack? Presence would certainly help get U.S. forces to a crisis area faster, but U.S. military presence overseas is declining, as is the number of military personnel in the United States who can be deployed. So compelling adversaries to stop what they are doing or planning by using military force against them may be a wise strategy in the post-Cold War world.

Historically, the United States has usually employed its military to compel enemies to change their behavior after a crisis began. The National Security Act of 1947 and its subsequent amendments have structured the U.S. security apparatus to react to crises rather than to prevent them. Given the nature of such post-Cold War threats as biological and chemical weapons, it may be time to consider preemption.

The preemptive use of military force is a difficult concept for many Americans to accept. It defies Americans' sense of fairness, proportionality, and the rules of warfare. As Brad Roberts points out:

Moral philosophy establishes that wars of self-defense are just, whereas wars of aggression are not. But there has long been a healthy debate about precisely what constitutes a war of self-defense. A mid-sixteenth-century scholar of just war wrote, "There is a single and only just cause for commencing a war . . . namely, wrong received." In our day Michael Walzer has argued, "Nothing but aggression can justify war. . . . There must actually have been a wrong, and it must actually have been received (or its receipt must be, as it were, only minutes away)."<sup>194</sup>

However, this view has not been universally held. Hugo Grotius wrote in 1625, "the first just cause of war . . . is an injury, which even though not actually committed, threatens our persons or our property."<sup>195</sup> To safeguard against wars of aggression, Grotius emphasized that it was essential to be certain about the enemy's intent to attack. Elihu Root said in 1914 that international law did not require the aggrieved state to wait before using force in self-defense "until it is too late to protect itself."<sup>196</sup> Interestingly, Walzer in *Just Wars* seems to contradict the statements quoted above by arguing that "states can rightfully defend themselves against violence that is imminent but not actual."

Roberts contends, and I agree, that there can be "no blanket reply to the question, is there a moral case for preemption. Some acts of preemption will be deemed just, others unjust."

In the case of preemption against biological and chemical threats, Roberts further argues that the strongest moral case for U.S. preemption exists under the following conditions:

- an aggressor has actually threatened to use his NBC weapons, has taken steps to ready the means to do so, and has specifically threatened the United States (including its territory, citizens, or military forces);
- those NBC weapons have been built in violation of international law;
- the aggressor's threatened actions invoke larger questions about the credibility of security guarantees or the balance of power within a region;
- the president has secured the approval of the U.S. Congress; and,
- the United States has secured the backing of the U.N. Security Council and any relevant regional

organization. The prudential tests of last resort, proportionality, and reasonable chance of success must also be met.<sup>197</sup>

I agree with the first four of Roberts' conditions but not with the last. Getting the backing of the U.N. and regional organizations would strengthen our moral position, but it may be impossible given China's reluctance to violate sovereignty under any circumstances and Russia's post-Kosovo habit of siding with rogue states like Iraq and Iran. And I believe that, as a matter of principle, the United States must never forego the option to act unilaterally.

Furthermore, the commonly held view that the U.S. public disapproves of preemption is not true. A good example is the 1998 bombing of a Sudanese chemical plant that was suspected of having ties to Osama bin Laden. Even after it emerged that the plant was probably making nothing sinister, public opinion in the U.S. was strongly in favor of the attacks.<sup>198</sup> Two-thirds of Americans approved the military strike, while only 19 percent were opposed.<sup>199</sup>

### Recommendations—International Threat.

Internationally, the United States is organized adequately to address the threat but must be prepared to operate in a less state-centric world. Our prohibition against negotiating with terrorists needs to be reevaluated, our reliance on the Chemical Warfare and Biological Warfare Conventions needs to take account of rogue and transnational actors, and the United States needs a capability to use its military preemptively.

Finally, as a soldier who never much liked wearing MOPP gear, I can only hope that the fielding of newly available protective equipment is accelerated and future improvements come quickly.

## Conclusion.

To summarize: threats from CBW are probably not as severe as some make out but nevertheless must be taken seriously because of the catastrophic potential of a chemical, and especially a biological, terrorist event. Of course, in preparing for these threats, personal freedoms inherent in our democracy should not be compromised, nor should the United States just throw money at the problem.

We all now recognize the increased danger of CBW. Rogue states, failed states, failing states, transnational actors, or even disloyal Americans could surreptitiously deliver one or several such weapons, at home or abroad. The Tokyo subway incident was not science fiction, and the Oklahoma City and World Trade Center bombings could just as easily have been CBW attacks. Anyone who doubts that terrorists can smuggle chemical or biological weapons into New York City should reflect that they could easily be disguised as a bag of cocaine or a brick of marijuana.<sup>200</sup>

Graham Allison has warned that defending America against CBW attack will require eternal, multi-layered vigilance. "As the most open society in the world, America will remain most vulnerable to attacks, especially weapons delivered surreptitiously. In the real world of the next quarter-century, dreams of an invulnerable America are fantasy."<sup>201</sup> Still, many things can be done. A Homeland Defense organization is one, a refocused IC is another. Simply putting a qualified person in a position to achieve unity of command would be a significant start. And from longtime allies faced with the same threat—Israel, the UK, and Canada—the United States should learn that the military can support domestic security operations without endangering civilian control. Protecting America's service personnel against biological and chemical attack is of paramount importance as is the ability to "preempt" those who would use biological and chemical weapons against U.S. forces and interests.

Neither complacency nor hysteria is called for, but rather a modest and sustained investment in intelligence and other countermeasures, from prevention to preemption to preparedness.

Individuals take out insurance policies all the time to hedge against disasters that will probably never occur. This is one case where the United States government can do the same—and be satisfied if the premiums are ultimately wasted.<sup>202</sup>

## CHAPTER 6 - ENDNOTES

1. Rod Stark, "Looking at the Nature of WMD Terrorism," unpublished paper, Southwest Missouri State University, Internet [http://www.inforwar.com/mil\\_c4i/st...\\_the\\_Nature\\_of\\_WMD\\_Terrorism.html](http://www.inforwar.com/mil_c4i/st..._the_Nature_of_WMD_Terrorism.html), August 30, 1999, p. 2.

2. John Ellis and Courtland Moon, "Dubious Allegations," *Bulletin of The Atomic Scientists*, May/June 1999, p. 70.

3. Ellis, p. 1. The authors base their conclusion on eight central arguments, each of which can be refuted by archival evidence and reasonable counterarguments.

4. Federation of American Scientists Web Page, "CW Use in Iran-Iraq War," [http://www.fas.org/irp/gulf/cia/960702/72566\\_01.htm](http://www.fas.org/irp/gulf/cia/960702/72566_01.htm). See also *Encyclopedia of Bioethics*, 2544; Physicians for Human Rights Web Site, "Research and Investigations: Chemical Weapons" <http://www.phrusa.org/research/chemical.html>; U.S. Department of State, Office of the Spokesman, Press Statement by James P. Rubin, Spokesman, "Anniversary of the Halabja Massacre," March 16, 1998, <http://secretary.state.gov/www/briefings/statements/1998/ps980316a.html>; Peter Sawchyn, "Scientist Details Effects of Chemical Attack on Iraqi Kurds (Evidence shows long-term genetic damage to Halabja residents)," USIS Washington File, April 27, 1998, [http://www.fas.org/news/iraq/1998/04/98042702\\_npo.html](http://www.fas.org/news/iraq/1998/04/98042702_npo.html).

5. Judith Miller, "U.S. Officials Suspect Deadly Chemical Weapons In Yugoslav Army Arsenal," *New York Times*, April 16, 1999, p. 1.

6. Steven Lee Myers, "Federal Commission Predicts Increasing Threat of Terrorism," *New York Times*, September 21, 1999, p. 1.

7. Christopher J. Castelli, "Homeland Terrorism, More Kosovos Ahead, Security Panel Warns," *Inside the Navy*, August 9, 1999, p. 1.

8. *Ibid.*
9. *Ibid.*
10. Milton Leitenberg, "False Alarm," *Washington Post*, August 14, 1999, p. 15.
11. Ehud Sprinzak, "Terrorism, Real or Imagined—What is the Real Threat, WMC or Car Bombs?" *Washington Post*, August 19, 1998, p. A21.
12. Brian Michael Jenkins, *The Likelihood of Nuclear Terrorism*, Santa Monica, CA: RAND Corporation, P-7119, July 1985, p. 6.
13. Nicholas Wade, "Germ Weapons: Deadly, but Hard to Use," *New York Times*, November 21, 1997, Internet, [www.mtholyoke.edu/acad/intrel/germ.htm](http://www.mtholyoke.edu/acad/intrel/germ.htm).
14. Bruce Hoffman, *Inside Terrorism*, New York: Columbia University Press, 1998, p. 198.
15. Jessica Stern, "Taking the Terror Out of Bioterrorism," *New York Times*, April 8, 1998, Internet [www.mtholyoke.edu/acad/intrel/stern.htm](http://www.mtholyoke.edu/acad/intrel/stern.htm).
16. Jessica Stern, *Loose Nukes, Poisons, and Terrorism: The New Threats to International Security*, June 19, 1996, p. 3.
17. William S. Cohen, "Preparing for a Grave New World," *Washington Post*, July 26, 1999, p. A 19.
18. *Ibid.* and Steve Macko, "FBI Says There is a Marked Increase in Number of Domestic WMD Terrorist Threats," *ERRI Daily Intelligence Report*, vol. 4, October 3, 1998, p. 276.
19. Chitra Ragavan and David E. Kaplan, "The Boom in Bioterror Funds," *U.S. News & World Report*, October, 18, 1999, p. 24.
20. Jessica Stern, *The Ultimate Terrorists*, p. 21.
21. *Ibid.*
22. Richard Preston, "Annals of Warfare—the Bio Weaponers," *The New Yorker*, March 9, 1998, p. 56.
23. *Ibid.*



24. *Ibid.*

25. *Ibid.*, p. 57.

26. Gideon Rose, "It Could Happen Here—Facing the New Terrorism," *Foreign Affairs*, March-April, 1999, p. 135.

27. "Expert: Russia Retains Biological Weapons Ability," *Dallas Morning News*, October 21, 1999, p. 1.

28. *Ibid.*, p. 134.

29. Robert Davis, "Rescuers Train for Prospect of Chemical War," *USA Today*, July 29, 1999, p. 8D.

30. Chris Seiple, "Consequence Management: Domestic Response to Weapons of Mass Destruction," *Parameters*, Autumn 1997, p. 120.

31. *Ibid.*

32. C. L. Staten, "Two Men Arrested With Possession of Anthrax," *Emergency Net News Service*, Online. [Http://emergency.com/lv-antrx.htm](http://emergency.com/lv-antrx.htm), August 30, 1999, p. 2.

33. Jessica Stern, *The Ultimate Terrorists*, Cambridge: Harvard University Press, 1999, p. 51.

34. "Expert: Russia Retains Biological Weapons Ability," *Dallas Morning News*, October 21, 1999, p.1.

35. *Ibid.*

36. Stephen A. Cambone, *A New Structure for National Security Policy Planning*, Washington DC: The Center for Strategic and International Studies, 1998, p. 113.

37. *Ibid.*

38. Rose, p. 131.

39. *Proliferation: Threat and Response*, Washington DC: Government Printing Office, 1996, p. 43.

40. Jessica Stern, "Loose Nukes, Poisons, and Terrorism: The New Threats to International Security," Unpublished paper, June 19, 1996, p. 11.

41. Bruce Hoffman, *Inside Terrorism*, New York: Columbia University Press, 1998, p. 205.

42. *Ibid.*

43. Rose, p. 135.

44. Ragavan and Kaplan, p. 24.

45. *Ibid.*

46. Harlan K. Ullman, "Who Will Listen, Who Will Lead," Unpublished manuscript, June 1998, p. 278.

47. Wesley Clark, interviewed at Mons, Belgium, March 8, 1999.

48. Ullman, p. 279.

49. *Ibid.* p. 280.

50. Bradley Graham, "Teamwork as Military Task," *Washington Post*, October 12, 1999, p. A17.

51. "Transforming Defense—National Security in the 21st Century," Report of the National Defense Panel, December 1997, p. 23.

52. *Ibid.*

53. *Ibid.* p. 25.

54. *Ibid.*

55. *Ibid.*

56. *Ibid.* p. 26

57. James Woolsey.

58. Al Gore, "Intelligence Community," *National Performance Review*, Washington DC: U.S. Government Printing Office, 1993.

59. Angela Rogers, *Changing Threat Environment and U.S. Intelligence Community: Challenges in the New Millennium*, Unpublished paper.

60. "Intelligence Community in the 21st Century," *Summary*, U.S. House of Representatives Permanent Select Committee on Intelligence, Washington DC, (no date), p. 2.

61. Gore, p. 9.

62. Morton H. Halperin, "What Should the National Security Act of 1998 Look Like," *U.S. National Security Beyond the Cold War*, Contemporary Issue Series No. 6, Carlisle, PA: The Clarke Center, 1997, p. 34.

63. *Ibid.* See also Richard A. Falkenrath, "Confronting Nuclear, Biological and Chemical Terrorism," *Survival*, Autumn 1998, p. 59.

64. *Ibid.*

65. "Hart-Rudman Commission: U.S. Faces Homeland Attacks," *Aerospace Daily*, October 6, 1999, p. 1.

66. Rose, p. 135.

67. Seth Carus, "Biohazard, Assessing the Bioterrorism Threat," *New Republic*, August 2, 1999, p. 14.

68. Ashton Carter, John Deutch, and Philip Zelikow, "Catastrophic Terrorism—Tackling the New Danger," *Foreign Affairs*, November-December 1998, p. 83.

69. *Ibid.* p. 84.

70. Halperin, p. 40.

71. *Ibid.*

72. *Ibid.*

73. Carter, p. 83-84.

74. Falkenrath, p. 59.

75. *Ibid.*

76. *Ibid.*

77. Carter, p. 84; and Falkenrath, p. 59.

78. Rose, p. 136.

79. *Ibid.* p. 119.

80. Jennifer Stinhaure and Judith Miller, "In N.Y. Outbreak, Glimpse of Gaps in Biological Defenses," *New York Times*, October, 11, 1999, p. 1.

81. *Ibid.*

82. Steinhauer, p. 1.

83. Chris Seiple, "Consequence Management: Domestic Response to Weapons of Mass Destruction," *Parameters*, August 1997, p. 120.

84. *Ibid.*

85. Russell, p. 205. See also Fred Bayles, "Anti-Terrorism Plans Falling Short," *USA Today*, October 13, 1998, p. 15A.

86. Seiple, p. 122.

87. *Ibid.*

88. *Ibid.*

89. Kurt A. McNeely, Assistant for Anti-Terrorism/Consequence Management, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, Interview, September 14, 1999.

90. Seiple, p. 124.

91. *Ibid.* Seiple explains that the FBI and consequence managers were able to work out an arrangement for sample collection at the Atlanta Olympics. However, it was never used. Interestingly, not until after the bomb attack at the Atlanta Olympics was the threat of biological contamination even considered by the authorities.

92. *Response and Recovery Terrorism Response Annex*, Federal Emergency Management Agency, Internet <http://www.fema.gov/r-n-r/frp/frpterr.htm>.

93. Gideon Rose, "It Could Happen Here—Facing the New Terrorism," *Foreign Affairs*, March-April, 1999, p. 136.

94. Carter, p. 90.

95. *Ibid.*

96. Willam S. Cohen, "Preparing for a Grave New World," *Washington Post*, July 26, 1999, p. A19.

97. Thomas R. Lujan, "Legal Aspects of Domestic Employment of the Army," *Parameters*, Autumn 1997, p. 83. The Navy is not specifically mentioned in the Posse Comitatus Act but has chosen to adhere to its constraints. The Coast Guard is not precluded from domestic operations by the Posse Comitatus Act.

98. *Ibid.* found in Congress, House of Representatives, Panel B, *Inquiry into Federal Law Enforcement Actions at Waco, Texas*, July 20, 1995, testimony of Brigadier General Walter P. Huffman, Assistant Judge Advocate General for Military Law and Operations, p. 14.

99. *Ibid.* p. 89.

100. Cohen, p. A19.

101. John J. Hamre, "U.S. Military Wants No Domestic Law Enforcement Role," October 5, 1999, p. 16.

102. *Ibid.*

103. Dennis M. McCarthy, "Joint Support for WMD Anti-Terrorism and Force Protection Planning," Briefing presented at the *WMD Response in the New Millennium Symposium*, Kirtland Air Force Base, New Mexico, July 21, 1999.

104. Greg Seigle, "USA Infighting Over Who Should Deal With Domestic WMD Attacks," *Jane's Defence Weekly*, July 7, 1999, p. 1.

105. "Regional Rapid Assessment Element Stationing Plans Announced," *DoD News Releases*, Office of the Assistant Secretary of Defense (Public Affairs), May 22, 1998, p. 1.

106. J. D. W. Parker, "USA Prepares to Treble Number of RAID Teams," *Jane's Defence Weekly*, June 2, 1999, p. 1.

107. Siegle.

108. Ron Laurenzo, "GAO: Time to Reassess Guard Anti-Terror Teams," *Defense Week*, July 6, 1999, p. 1.

109. Bradley Graham, "Sneak-Attack Detectives Prepare to Prowl," *Washington Post*, August 28, 1999, p. 3.

110. *Ibid.*

111. Lorenzo.

112. *Ibid.*

113. *Ibid.*

114. Jonathan Pate, Center for Nonproliferation Studies, Monterey Institute of International Studies, Interview, February 12, 1999. See also "Agency Structure for Terrorism Response—Federal Funding to Combat Terrorism," *Chemical and Biological Resource Page*, Center for Nonproliferation, Internet <http://www.cns.miis.edu/research/cbw/response.htm>.

115. Zeev Livne, Israeli Defense and Armed Forces Attache, Interview, October 8, 1999, Washington DC.

116. *Ibid.*

117. *Ibid.*

118. *Ibid.*

119. *Ibid.*

120. "The Home Front is Prepared," *Israel Wire*, December 18, 1998, Internet, <http://www.israelwire.com/Ira/981218/9812184.html>.

121. "Enough Gas Masks for Everyone," *Israel Wire*, December 18, 1998, Internet, <http://www.israelwire.com/Ira/981218/981282.html>.

122. Livne.

123. *Ibid.*

124. Geoff Simons, *Iraq—From Sumer to Saddam*, second ed., New York: St. Martin's Press, 1996, p. 320.

125. *Ibid.* See also, Julie Flint, "Saddam Killing Shias 'Daily'," *The Observer*, October 4, 1992.

126. Neil C. Livinstone, "Proactive Responses to Terrorism: Reprisals, Preemption, and Retribution," *International Terrorism—Characteristics, Causes, and Controls*, Charles W. Kegley, Jr., ed., New York: St. Martin's Press, 1990, p. 225.

127. *Ibid.*

128. *Ibid.*

129. *Ibid.*

130. David C. Veness, Assistant Commissioner Specialist Operations, Metropolitan Police Services, London. Interview, March 5, 1999.

131. Mark Kesselman, Christopher S. Allen, David Ost, Joel Krieger, Stephen Hellman, and George Ross, *European Politics in Transition*, 3rd edition, Boston: Houghton Mifflin Company, 1997, p. 95.

132. Harlan Ullman, Interview, November 7, 1999.

133. Veness.

134. Kesselman, p. 84.

135. *Ibid.*

136. *Ibid.* p. 85.

137. "The SAS Raid on the Iranian Embassy," *Overlord—Special Forces and Counterterrorism*, Internet, <http://home.istar.ca/~overlord/welcome.html>.

138. "Operation Nimrod—The Embassy Siege," *Special Forces of the World*, Internet.

139. <http://home.istar.ca/~overlord/raidiran.html> and <http://www.specialforces.dk/reallife/nimrod.htm>.

140. Dr. Ray Raymond, Consular Officer, British Consulate, New York, Interview, September 27, 1999. Rules are not hard and fast with regards to the classification and the classification can change within the life span of the crisis.

141. Dr. Ray Raymond.

142. T. J. Grant, "Training on Rules of Engagement in Domestic Operations," unpublished paper, Canadian Defense College, Internet, <http://www.cfcsc.dnd.ca/irc/amsc/amsc1/014.html>, p. 1.

143. *Ibid.*

144. [http://www.dnd.ca/menu/legacy/defend\\_e.htm](http://www.dnd.ca/menu/legacy/defend_e.htm).

145. [http://www.dnd.ca/menu/legacy/defend\\_e.htm](http://www.dnd.ca/menu/legacy/defend_e.htm).
146. Sean M. Maloney, "Domestic Operations: The Canadian Approach," *Parameters*, Autumn 1997, p. 143.
147. *Ibid.*
148. *Ibid.*
149. *Ibid.*
150. [http://www.dnd.ca/menu/legacy/helping\\_e.htm](http://www.dnd.ca/menu/legacy/helping_e.htm).
151. Maloney, p. 144.
152. *Ibid.*
153. *Ibid.*, p. 148.
154. *Ibid.*
155. Seiple, p. 119.
156. John Ellis, "What the U.S. Must do to Combat Biological Weapons," *Boston Globe*, December 10, 1998, p. A. 31.
157. Stern, p. 131.
158. *Ibid.*
159. James Risen, "To Bomb Sudan Plant or Not: A Year Later, Debates Rankle," *New York Times*, October 27, 1999, p. A14.
160. John M. Goshko, "Sudan to Sign Anti-Terrorism Accords and Join Chemical Warfare Ban," *Washington Post*, May 22, 1999, p. 20.
161. Lewis A. Dunn, "Proliferation Prevention: Beyond Traditionalism," *Weapons of Mass Destruction: New Perspectives of Counterproliferation*, William H. Lewis and Stuart E. Johnson, eds., Washington, DC: National Defense University Press, 1995, p. 37.
162. *Ibid.*
163. Deborah R. Lee, "Protecting Americans at Home," *Defense Link*, March, 19, 1998, p. 2. Online. [Http://www.defenselink.mil/other\\_info/deblee.html](Http://www.defenselink.mil/other_info/deblee.html).



164. Mercier, p. 108.

165. *Ibid.*

166. "Operations Other Than War Volume II—Disaster Assistance," *Center for Army Lessons Learned Newsletter*, no. 93-6, October 1993, p. IX 2.

167. Brian Hawtin, Deputy Policy Director, Assistant Under Secretary of State (Policy), Ministry of Defense, Interview, March 4, 1999.

168. H. Allen Holmes, "Domestic Preparedness: U.S. Responses Need Tuning," *Defense Viewpoint*, Vol. 13, No. 33, March 26, 1998, p. 5. Online. [www.defenselink.mil/speeches/1998/s19980326-holmas.html](http://www.defenselink.mil/speeches/1998/s19980326-holmas.html).

169. Carter, p. 91.

170. Maloney, p. 150.

171. *Ibid.*

172. Peter Grier, "New Roles For the Guard and Reserve," *Air Force Magazine*, November 1999, p. 17.

173. Stern, p. 143.

174. James Q. Wilson, *Bureaucracy—What Government Agencies Do and Why They Do It*, New York: Basic Books, 1989, p. 190.

175. "U.S. Weapons Fight May be Reorganized," *Philadelphia Inquirer*, July 7, 1999, p. 1.

176. *Ibid.*

177. C. Mark Brinkley and Gordon Lubold, "Corps' Bio Force Just Not Enough," *Marine Corps Times*, March 29, 1999, p. 13.

178. Ernest R. May, "Intelligence: Backing Into the Future," *Foreign Affairs*, Summer 1992, p. 65.

179. Ellis.

180. May, p. 72.

181. *Ibid.*

182. *Ibid.*

183. Jane Holl, multiple discussions.

184. Barbara Starr, "USA's Covert Squads to Counter WMD," *Jane's Weekly*, March 11, 1998, p. 12.

185. Richard W. Perry and Stephen R. A. Robinson, Rock Island Arsenal, Interview, May 27, 1999.

186. John M. Donnelly, "Majority of Military Gas Masks in Survey 'Critically' Defective," *Defense Week*, June 21, 2000, p. 1.

187. *Ibid.*

188. Chuck Vinch, "Services Complete Chemical Suit Check," *European Stars and Stripes*, April 6, 2000, p. 4.

189. *Ibid.*

190. [http://www.cotf.navy.mil/code70/73\\_jslis.htm](http://www.cotf.navy.mil/code70/73_jslis.htm).

191. Stansfield Turner, *Terrorism and Democracy*, Boston: Houghton Mifflin Company, 1991, p. xii. Actually Admiral Turner makes the argument that the United States will negotiate with terrorists. See Chapter 26, "We Will Make Deals."

192. "Weapons of Mass Destruction," *Great Decisions*, 1999, p. 51.

193. *Ibid.*, p. 52.

194. Brad Roberts, "NBC-Armed Rogues: Is there a Moral Case for Preemption?" *Close Calls: Intervention, Terrorism, Missile Defense, and 'Just War' Today*, Elliott Abrams, ed., EPPC-March, 1998, p. 11.

195. Hugo Grotius, *The Law of War and Peace*, book 2, chapter 1, section 2.

196. Elihu Root, "The Real Monroe Doctrine," *American Journal of International Law* 35, 1914, p. 427.

197. Roberts, p. 13.

198. "Excerpts: U.S. Editorials assess impact of Anti-Terrorist Strikes," *USIS Washington File*, [http://www.fas.org/man/dod-101/ops/docs/98082307\\_tpo.html](http://www.fas.org/man/dod-101/ops/docs/98082307_tpo.html), June 14, 2000, p. 1-6.

199. John Diamond, "US Strikes Tougher Stance Against Terrorism," *Cnews* August 21, 1998, [http:// www.canoe.ca/CNEWSStrike AtTerrorism/aug20\\_us.html](http://www.canoe.ca/CNEWSStrikeAtTerrorism/aug20_us.html).

200. Graham Allison, "Nuclear Lessons," *Boston Globe*, October 27, 1999, p. 23. The author hopes Dr. Allison won't object to my substituting chemical and biological for nuclear.

201. *Ibid.*

202. Rose, p. 137.

## CHAPTER 7

### INFRASTRUCTURE WARRIORS: A THREAT TO THE U.S. HOMELAND BY ORGANIZED CRIME

Thomas A. Johnson

Two very important databases, one collected by the Terrorism Research Center in cooperation with Georgetown University and the second by Carnegie Mellon University's Coordination Center, each reveal a similarity between cyberterrorism and cybercrime by organized crime. The striking similarity is our fear and apprehension of each despite few recorded incidents of either.

The number of incidents reported to the CERT Coordination Center from 1988 to March 2000 is over 30,000.<sup>1</sup> Indeed, the number of incidents reported does not address or reveal any pattern of cyberterrorism or cybercrime by organized criminals. It is a fact that CERT was organized to report on security vulnerabilities and to issue advisories while also maintaining a log of incidents reported. While the CERT Center is a most valuable asset, it would be instructive to receive more information such as John D. Howard's Ph.D. dissertation, "An Analysis of Security Incidents on to Internet 1989-1995," where Howard proposes a taxonomy of computer and network attacks and classifies attackers into six categories with four categories of primary motivation and six sets of tools. The development of Howard's taxonomy of Internet attacks is an important research tool having great utility in analyzing criminal activity by organized crime in the foreseeable future.

Computer and Network Attack Taxonomy <sup>2</sup>		
<u>Attackers</u>	<u>Tools</u>	<u>Objectives</u>
Hackers	User Command	Corruption of Information
Spies	Script of Program	Disclosure of Information
Terrorists	Autonomous Agent	Theft of Service
Corporate Providers	Tool Kit	Denial of Service
Professional Criminals	Distributed Tool	
Vandals	Data Top	

Another fascinating classification proposed by Dorothy E. Denning in her excellent paper, "Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" suggests the importance of the Internet and how it can be an effective vehicle for creating coalitions among various groups. Denning presents three classifications of activity:

1. Activism as the normal nondisruptive use of the Internet in support of an agenda or cause.

2. Hactivism (the marriage of hacking and activism) covers operations that use hacking techniques against target internet sites with the intent of disrupting normal operations but not causing serious damage. Examples are Web sit-ins and vertical blockades, automated E-mail bombs, Web hacks, computer break-ins and computer viruses and worms.

3. The final category, cyberterrorism, refers to the convergence of cyberspace and terrorism. This covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage.<sup>3</sup>

Denning's classification emphasizes the enormous potential for both organized crime and cyberterrorists to use the Internet to their great respective advantage.

Based upon a review of over 110 reported computer and information system attacks included in the Georgetown University's *Terrorism Research Center, Information Warfare Database*;<sup>4</sup> as well as Philip Osburn's paper on the *Terrorist Threat*, it is clear that our media has exaggerated a sense of cyberterrorist attacks. A potential for such cyberterrorism does exist, but as the Naval Postgraduate School study suggested, cyberterrorism is a challenge for the future. We believe the potential for cyberterrorism is within the reach of terrorist organizations, and that many of these terrorist organizations are only now becoming aware of the awesome potential for use of information technologies in furthering their respective objectives. In reality, this should not be a surprise as our world's leading educational institutions have only recently embarked upon a concentrated effort to adapt these technologies to distribute their respective mission via "distance education" strategies. If institutions of higher education have only recently discovered the potential of information technologies, there is no reason to believe that terrorist organizations would have made this discovery any earlier, and more importantly, even less reason to suspect they are also not on the threshold of materially refocusing their *modus operandi* and attack structures.

Philip Osburn's excellent paper on the terrorist threat reviews the literature and reports on only two cyberterrorist attacks, the first being the TAMIL guerrillas Liberation Tigers of Tamil Eelam (LTTE), which performed an E-mail bombing attack to create a denial of service on Sri Lankan embassies. The second cyberterrorist attack was committed on behalf of the Zapatistas by a group of Italian sympathizers against the Mexican Government and Army.<sup>5</sup>

While there exists few recorded cyberterrorist attacks and few examples of organized cybercrime, we wish to

emphasize the potential threat that each will create. Furthermore, we suggest that it is only a matter of time before these respective groups tool up to the task.

Perhaps one of the most important and provocative research reports to emerge on this subject is the *Cyberterror: Prospects and Implications* report by John Arquilla, *et. al*. The conceptual framework and taxonomy presented an opportunity to view both cyberterrorist and organized criminals' cybercrime in a new and enlightened fashion.

Their taxonomy, described below, provides a unique methodology for gathering and analyzing data which should provide for more precise assessments of both threats in the future.

*Simple-Unstructured:* The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.

*Advanced-Structured:* The capability to conduct more sophisticated attacks against multiple systems or networks and possibly to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control and learning capability.

*Complex-Coordinated:* The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organizational learning capability.<sup>6</sup>

The opportunity to utilize and refine the three presented taxonomies to analyze both cyberterrorism and the cybercriminal activity in which organized crime will no doubt engage, should assist us in developing strategies for controlling each event.

As we examine these terrorist groups, we should focus upon how each one either uses or anticipates the use of information systems. We wish to explore to what extent, if any, these groups use information systems to recruit other individuals into their cause. We hypothesize that terrorist organizations will use information systems to seek greater legitimacy within their society while, at the same time, enhancing their opportunity to recruit more participants and members to their cause. The use of information systems to more efficiently "market" their message and their cause may well confuse many people who otherwise would remain in more established opposition to the terrorist group. We also will be interested in exploring if and how any of these terrorist groups attempt to more "surgically" disrupt their targets by use of information technologies. Finally, what methods of collaboration, if any, might be used by terrorist organizations mutually participating through information systems in joint activities designed to disrupt their targets.

Several similarities between cyberterrorism and organized crime in terms of the threat to our U.S. homeland is discussed in the RAND Research Review of Fall 1995, where it is observed how inexpensive it is to wage an Information War, as the acquisition of information weapons neither require vast financial resources or state sponsorship. Indeed, all that is required is a computer, a network, an internet service provider, and various software tools. Since the global nature of this environment blurs the boundaries of cyberspace, it makes enforcement methods much more difficult.<sup>7</sup>

The threat to our U.S. homeland by infrastructure warriors who may be controlled by or working for organized crime is a very real threat with profound consequences. There exist a growing number of cyber-assault weapons that can easily target both E-Government and E-Commerce activities and programs. The easy availability of these cyber-assault weapons on the worldwide web makes the cost and increased opportunity of attacks very efficient and potentially effective. To further exacerbate the problem,



there exists a growing number of people with the skill sets capable of implementing the attack scenarios; all that remains is for organized crime and drug networks to locate the people with sufficient skills to (1) introduce a vision for moving organized crime into cyberspace, and (2) for locating and engaging people with the skill sets to acquire, develop, and utilize the number of cyber-assault tools to effect the end goals of organized crime.

### Cyber-Tools and Strategies Available to Organized Crime.

There exists a number of cybertools and cyberstrategies to organized crime to invoke against legitimate business. These cyber-assault tools will also make the government's job of controlling organized crime much more difficult. A brief description of the cyber-assault weapons and cyber strategies with which law enforcement and military investigative services will be challenged follows in this section.

Encryption, which will assure far greater confidentiality of organized crime plans and discussions. The use of encryption by organized crime and drug networks will make it more difficult for investigative agencies to obtain evidence of criminal activities. Encryption will also make it profoundly more difficult to obtain intelligence vital to the criminal investigation. Also, encryption of organized crime plans makes it difficult to avert terrorist type attacks. Since gathering foreign intelligence about different group activities against the U.S. is vital to our national security, the use of encryption by organized criminal elements is a direct threat to our homeland.<sup>8</sup>

Other effects of encryption range from precluding our investigations to affecting them by delay and increased costs. Unbreakable encryption may cause investigators to implement alternative undercover operations which may be more dangerous to law enforcement officers; more

expensive; and potentially more invasive to the subject's privacy.<sup>9</sup>

Indeed, the debate surrounding the "clipper chip" proposal and the issues of balancing privacy with the requirements that exist in a democracy has been long and heated. The advent of free downloadable encryption programs on the web has made law enforcement's concerns quite realistic.

Denning and Baugh observed that "we are at the leading edge of what could become a serious threat to law enforcement and national security: the proliferation and use of robust digital encryption technologies. These technologies will be unbreakable, easy to use, and integrated into desktop applications and network services, including protocols for electronic mail, web transactions and telephony."<sup>10</sup>

Drug cartels, particularly in Columbia, have utilized encryption to obfuscate law enforcement's ability to investigate their operations. Also, the Drug Enforcement Administration (DEA) has reported that the cartel has utilized mainframe computers and even has used DEA telephone lines to for their illegal business activities.

Cryptoviral extortion has been reported by Denning and Baugh to have occurred to at least nine businesses in London in which cryptoviruses enciphered the data, financial records, and files and in effect encrypted the companies financial records. The companies were contacted by the responsible hackers and offered the decryption key for \$150,000.<sup>11</sup> I am familiar with one case similar to this on the East Coast. Consequently, this could be a substantial threat if ever adopted by organized crime on a large scale.

Steganography or its use of S-tools and other tools to hide messages or digital images within pixels of an otherwise innocuous photograph or painting will provide organized crime a potent delivery system of child pornography to pedophiles.

The expanding capability of our electronic hard drive storage system has provided a most fertile ground for organized crime to process incredible amounts of data in their gambling operations. A recent case occurring in California and Kansas involved the illegal gambling operation in which investigators were confronted with 100 terrabytes of data.

On-line pornography has been a market, which has not been fully targeted by organized crime. It will only be a matter of time before they intrude on the shady operators and web entrepreneurs who have made millions of dollars in this area. This is a fertile market place that is first and foremost global; 24 x 7; with a pattern of repeat customers who return multiple times each day at \$30 to \$40 per occasion. The confusing pattern of laws from nation to nation, and the need for targeting search warrants in multiple jurisdictions, will make this an attractive organized crime market. The web-entrepreneurs that have chartered out the numerous web sites dealing with pornography will become quite valuable to organized crime pushing into this arena.

Packet sniffers to identify passwords and identification of computer users will become a marketplace for a variety of organized crime blackmail and extortion activities. Other cybertools such as anonymous remailers; network scanners, i.e., satan and other such tools will also be most useful to organized crime's efforts to disrupt legitimate business enterprise.

Terrorists groups operating within the United States and targeting U.S. business have included Ramsey Yousef and others who have been apprehended with lap tops that have utilized encryption to render their plans unreadable to law enforcement authorities.

The U.S. concern regarding chemical and biological weapons was taken to a new level by the Aum Shinri Kyo terrorist group in Japan when it was discovered their cult had stored their records on computers encrypted with a very

secure encryption format (i.e., RSA). The encrypted files contained evidence that included plans to deploy weapons of mass destruction in the United States.<sup>12</sup>

Denial of service attacks, which have principally been used by hackers, will provide an incredibly lucrative market to organized crime. This could well become the cyberspace "protection market" that will pale into insignificance the "protection" rackets of organized crime in the 1920s and 1930s.

In summary, the challenge that confronts our criminal justice system is to provide the skilled personnel who have the capabilities to confront the next generation of organized cyber criminals. This will entail training of our law enforcement personnel in the areas of computer science, law and forensic investigation.

## CHAPTER 7 - ENDNOTES

1. Carnegie Mellon Software Engineering Institute CERT Coordination Center, CERT/CC Statistics 1988-2000, [www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html).

2. John D. Howard, *An Analysis of Security Incidents on the Internet: 1989-1995*, Carnegie Mellon University Ph.D. Dissertation, Copyright by John D. Howard, 1997, Chapter 6, pp. 7-9, [www.cert.org/research/jhthesis/chapter6.html](http://www.cert.org/research/jhthesis/chapter6.html).

3. Dorothy E. Denning, *Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Internet and International Systems: Information Technology and American Foreign Policy Decision-Making Workshop, pp. 1-2.

4. The Terrorism Research Center, in cooperation with Georgetown University, Information Warfare Database, 1982-2000.

5. Philip Osborn, *The Terrorist Threat: An Examination of Terrorist Groups and the Threat to the National Information Infrastructure*, a graduate paper for CJ-625, University of New Haven, December 1999, pp. 7, 10.

6. Arquilla, Tucker, Nelson, Choi, Iacobucci, Mitchell, and Gagnon, *Cyberterror: Prospects and Implications*, Monterey: Center for the Study of Terrorism and Irregular Warfare, March 2000, pp. 7-8.

7. Ann Shoben, Editor, "Information Warfare: A Two-Edge Sword," *Information War and Cyberspace Security*, RAND Research Review, Fall, 1995, Vol. XIX, No. 2, p. 3.

8. Dorothy E. Denning and William E. Baugh, *Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism*, National Strategy Information Centers, U.S. Working Group on Organized Crime, July 1997, pp. 13-14.

9. *Ibid.*, p. 15.

10. *Ibid.*, p. 1.

11. *Ibid.*, p. 5.

12. *Ibid.*, p. 4.

## CHAPTER 8

### THREAT OF CIVIL UNREST AND INSURRECTION

William A. Navas, Jr.

It has been said that the primary duty of government—of organized government—is to provide for the safety and security of its citizens. Now we see internal threats that challenge the sense of security that we have enjoyed for decades during the Cold War, when we perceived our threats to be external rather than internal. So we begin to see an emergence of some threats that we can define as “clear and present dangers.” The title of this year’s conference, “. . . to insure domestic Tranquility, provide for the common defence,” is very timely in the face of this.

And also, the fact that we have this conference here at Carlisle, like Dr. Urwin said this morning, is also very appropriate because it was here in October of 1794 where President Washington for the first time federalized the militia—elements of the New Jersey, Maryland, Virginia, and Pennsylvania militias—to enforce the laws of the Union and quell the Whiskey Rebellion. And it was here at Carlisle General Washington, then President Washington, as commander-in-chief, took to the field and reviewed the troops. So some things do not change, I guess.

What I would like to do today is address the threat of civil unrest and insurrection in this new environment. It seems that today you cannot attend one of these conference without hearing, *ad nauseam*, the term “Post Cold War” or “End of the Cold War.” But again, we need to deal with that because what we are dealing with are the effects of the end of the Cold War and what that entails for the world in general, and for the United States in particular, by creating some unprecedented tensions in the international and

domestic environments. There is an excellent book written by Thomas Freidman, *The Lexus and the Olive Tree*, wherein he posits that “globalization” is a system that is replacing the Cold War as a system, not only in military terms but as political and economic systems as well. And this perhaps is what is causing some of the turmoil that we are experiencing.

So I am going to give you, very briefly, the situation in the United States today—first, as a nation of conflicts (and I will explain what I mean by that); second, as the only remaining superpower (what that entails and what that means); and, third, why we are at a critical juncture. And you will see how these three factors are going to converge into giving us some challenges and some opportunities.

The United States is a nation of conflicts. Like I said, Globalization is replacing the Cold War as a political/military/economic system. In fact, it is creating a global village, if you will. It is replacing the old system at the same time that we are experiencing, on the other hand, an explosion of communications and other technological changes that are creating even more tensions in the old system. The perception also, particularly in the United States, that only some are benefiting from this new economic boom and new technological opportunities, can create some tensions, especially for those who feel either left behind or brutalized by this. So what you see is a new conflict of constituencies. Not only the old majority versus minority or along racial lines, but we are seeing basically the conflicts of interest group versus interest group, gender coalitions, religious, ethnic, and life-styles conflicts that are coming out there because of this new found information and freedom.

Also the fact that some people feel that some of our systems are deteriorating—that the trust of the American people in some of our systems is not there—creates more tension. This is not a case for political reform. I mean, God knows, enough is said about that in an election year, we are

going to hear more of that. But that is a fact that needs to be considered, because we are not as homogenous as we thought we were or some sectors would like us to be.

The second issue is the fact that we are the only remaining superpower. Dr. Henry Kissinger stated in a recent article in *The Washington Post*, and I quote,

The end of the millennium coincides with the moment when America is preeminence turned into predominance. Never before has a single country achieved a comparable ascendancy on a global basis and in so many fields of endeavor, from weaponry to economics, to entrepreneurship, to even pop culture.

However, that supremacy, that leadership for the past 10 years that everyone took for granted—we in the United States, and even around the world—is starting to see some fraying. We see other countries, Russia, China, and India, are starting to challenge U.S. pre-eminence. Someone said that the burden of power is having to wield it. And, like Kissinger said, American foreign policy cannot careen between overcommitment and abdication. We are trying to come to grips in our country with what is a logical foreign policy for the United States. We need one that is understood by friend and foe alike, one that balances between avoiding being heavy-handed on one side of the equation, and on the other creating a leadership vacuum that can bring into imbalance this delicate subject. So the issue here is, unilateral dominance—hegemony—cannot be sustained indefinitely, and, as history has taught us, in the end it can be more harmful than beneficial to our national interests. So we, as the only remaining superpower, still have to come to grips with what is going to be our role.

Then the third issue here is that we are, again, at a critical juncture because we are not only enjoying economic growth and global superiority at the same time, but we are making a lot of progress in some other areas of human endeavor, like in medicine and technology. The end of the Cold War also has ushered a period of domestic self-



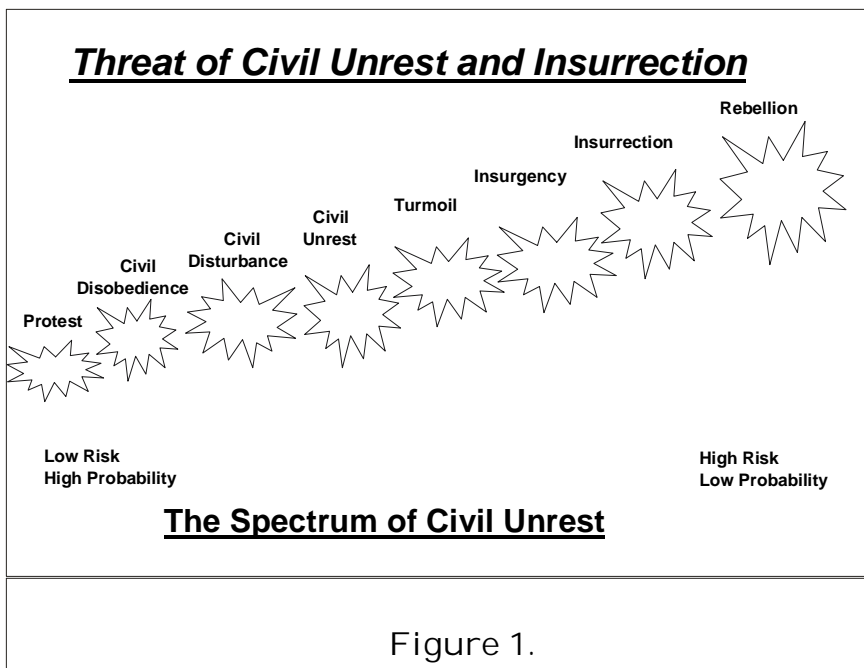
examination. It is very interesting that, for a long time, people had looked at the Commerce Department's *Index of Leading Economic Indicators* to spot trends in the economy. And recently Mr. William J. Bennett has been publishing an *Index of Leading Cultural Indicators*.

It is kind of a bellwether to see how well we are doing domestically in issues such as crime, family issues, education, youth behavior, popular culture, and religion—like a report card of how are we doing. And this is helpful because it is going to start putting the spotlight on some elements of the population that feel left behind and losing the confidence that democracy is taking care of all in our country. Not that we can take care of every single need or expectation, but there must be a feeling from the citizens of the legitimacy of their government and that it is acting in the best interest of the whole.

This is helpful because, if there are elements of the population that feel disenfranchised and “left behind” in this new era of prosperity and growth, then manipulation by those external elements inimical to our interests could very well plant the seeds of unrest in our society. So that is how we see the situation today, in both the domestic and international arenas. This is how we stand at the end of the Cold War.

I borrowed from the old Cold War spectrum of conflict and adapted it to the threats of civil unrest and insurrection. (See Figure 1.) If you recall, we always had the low risk/high probability, low intensity conflict on one side, and then we went to the high risk/low probability global thermonuclear war on the other side. So what I have done here is arranged in order of severity, if you will, the different threats that we have, going from peaceful protest on one end, to rebellion on the other. And what I would like to do is, not to define these events, but illustrate and give examples of what we understand each of those events to mean.

Let me start with **protest**. It is the most benign of the forms of civil actions. It is basically even healthy in a



democracy because we provide for those mechanisms. And protest could go from the sublime to the ridiculous, from the Million Man March in Washington, to the broccoli producers protesting in front of the White House because President Bush said he did not like broccoli. It goes the full gamut. And again, this is something that, if handled well, it is healthy to democracy.

The next level is ***civil disobedience***. And again, when peaceful and orderly, although it might violate some statutes or ordinances, it could be a very powerful way for a group to deal with their issues, especially groups that feel disenfranchised or that they do not have the mechanisms to make their views seen. One of the current issues is the case of the citizens of Vieques, Puerto Rico, and the U.S. Navy, where the issue is not the Navy bombings *per se*, but it is the issue of people who feel disenfranchised because they do not have the political power of the vote and representation to resolve the issue. So the way they deal with this situation is by civil disobedience, by physically occupying a position on

the bombing range to prevent the Navy from resuming the training exercises.

The next level in that spectrum is ***civil disturbance***. This is the first form of violent manifestation. It is characterized by anger, violence, and lawlessness. Normally it evolves around a single issue or event, but mob mentality and a sense of anonymity also takes over, and then you have a very ugly situation. And again, one of the recent examples are the Los Angeles riots of 1992 that turned into a couple of days of near anarchy in the wake of the Rodney King beatings by the police.

***Civil unrest*** develops over a period of time with wide geographic dispersion and can trigger episodes of protest, civil disobedience, and civil disturbances that can escalate. Although it centers on a single issue, it tends to act as a magnet to attract other causes. The best example of this is the later years of the Vietnam War with the United States and the Civil Rights Movement. They were times of civil unrest with episodes of different types of violence and protest.

I see ***Turmoil*** as some of those episodes resulting from civil unrest. It is the "flash-in-the-pan" type event. An example is the university riots during the Vietnam War, in particular Kent State (which was discussed this morning), where things reach a flash point, get out of hand, and you have violent acts.

***Insurgency*** is a lot more serious; it is a condition of revolt against the government. It is less than organized revolution, and it is not recognized as belligerency. The current militia groups and fringe elements, such as the Nationalists in 1950 in Puerto Rico, are examples of this type of elements that uses force and violence to protest against an established system.

***Insurrection*** is basically revolting against civil authority, an established government, by violent means. Fortunately, we do not have any recent examples in the

United States, but Chechnya and East Timor come to mind as examples of insurrection.

And then we have **revolution**, which is the open opposition to those in authority by means of force. Our Civil War, at least from the Union standpoint, is an example of that.

So we have seen all of those different levels. Now what are the causes or the trigger mechanisms that can generate these actions? The list abounds, but let me mention a few. The first is **relativism**. The absence of sound public policy is a significant threat; and relativism, it has been called, euphemistically, political correctness, it is tolerance, it is acceptance, and it is accommodation. The issue is that it tends to blur the right and wrong on public policy, and this creates a sense that—if it is politically accepted, if you do not want to alienate a group—it is okay. And this prevents, particularly our elected officials and those appointed officials who work for elected officials, from doing what is right. They are reluctant to “call it like it is” and thus prevents these officials from “telling the Emperor he has no clothes.”

Then there is **Apathy**. A recently conducted CNN poll discovered that only 49 percent of the registered electorate participated in the 1996 presidential elections. When you consider that only about 56 percent of the eligible people are registered, this situation is something where we have to be very, very careful. If you project that trend, you could almost predict a collapse of our electoral system.

There is **Fragmentation** because we are no longer a nation of immigrants willing to come and be assimilated into the melting pot. The civil rights movement, globalization, ethnic pride, religious and cultural diversity, world communications, and ease of travel have created what we could define as “commuting immigrants” that have “broken the melting pot.” We must understand these dynamics and capitalize in the core values of our democratic system to become “the ties that bind.” The old “melting pot”

can become the new “salad bowl,” bound together by the “dressing” of enduring American values. But this is not predestined. We need the political leadership and will to establish this new vision for America. We cannot go back and long for things that are not there anymore. If we do, we could very well be planting the seeds of unrest ourselves.

And then, of course, you have **Information, Media, and Communications**. We talk a lot about the CNN factor. I think that when you are dealing with 24-hour news coverage, elected officials are forced to make decisions that should take a lot more time and analysis because of the perceived notion that they need to have their answer or their reaction at the next news cycle, or they will be perceived as hesitant or indecisive. That has a potential for disaster. Can you imagine the Vietnam era’s civil unrest period in today is CNN and Internet “chat rooms” environment?

That would have been disastrous. Or, on second thought, the war might have ended sooner! In any event, the explosion of communications is a factor that we need to take into account.

Two quick examples are first, Seattle, World Trade Organization meeting, December 1999—I do not need to go into details. There were a lot of arrests, and it turned ugly. It was supposed to be a very peaceful protest of people—well meaning individuals dealing with human rights, with animal rights, with this, and the other. Then the Diallo Verdict in New York City in March 2000, which had the potential of turning very ugly, was very peaceful because the African-American leadership there was very measured in their way of protesting.

Although it is probably politically incorrect to talk about Elian (González), you need to talk about him. That case was a classic example of what can happen if not handled correctly. It had extensive media coverage, it was highly visible, emotionally charged, and had an external environment and a political dimension (both foreign and

domestic). It was a conflict of values, traditions, and customs on one hand; and the perception on the other of the authorities being heavy-handed. The same thing, you could say, as potential flash points, for example, the Confederate Flag issue in South Carolina, the IMF meeting in Washington, DC, in April, and again, the Navy/Vieques issue in Puerto Rico.

In conclusion, we have seen there is a present danger because, first, the unprecedented global changes that we have discussed have created new tensions and exacerbated some latent ones. This happens at a time when the United States emerges as the only superpower, and there are some elements that want to challenge that pre-eminence.

Second is the fact that a large sector of the American people has lost confidence in some of the systems—the political system, the retirement system—and traditional family values are being challenged.

And third, we have become a lot more diverse, so we have a lot more potential for conflicts between different interests, whether they are ethnic, family, or whatever.

So we conclude that, in this environment, the threat of civil disturbances is high. I am afraid we are going to see a lot of that. How we deal with that threat, and how we prepare for it can minimize the risk. The threat for unrest and insurrection is low, but, due to the high risk it presents and because some external factors and elements can be facilitators, it needs to be closely monitored for the severity of the consequences.

So in closing, I would like to end with a quote from Mahatma Gandhi. Our public policies ought to heed his advice. He stated that there are the “seven blunders of the world that can cause violence.” They are:

- Wealth without Work
- Pleasure without Conscience

- Knowledge without Character
- Commerce without Morality
- Science without Humanity
- Worship without Sacrifice, and
- Politics without Principle

# CHAPTER 9

## MISSILE DEFENSE

John Costello

I am going to be a little bit different today in terms of how I am going to talk to you about National Missile Defense and how it relates to homeland defense. I will attempt over the next few minutes to give you an honest assessment of where we stand, because you certainly will not get that from anything you read in the press.

I wear two hats. I am a Title 10 Commander, if you will, for General Eric Shinseki. The Army Space and Missile Defense Command is a major command of the United States Army responsible for technology development, testing, and fielding of a host of various missile defense and space related equipment. I am also a component commander to U.S. Space Command out in Colorado Springs, Colorado, where I command the Army Space Forces, those young men and women who work around the world doing our part of the space business. The National Missile Defense (NMD) system obviously takes up a lot of my time in that it is both a Title 10 responsibility, since the Army is the lead Service for the ground based element of the National Missile Defense program, and since ultimately I will command the Army forces that man this system should the President of the United States make a decision to field this system.

### Historical Background.

Well, as you know, the defense of the United States is and has always been a soldier's most sacred responsibility. From 1775 the Army has played a pivotal role in defense of the homeland. In 1794 the Congress charged the Army to build and staff coastal defense forts. As the threat changed over the centuries from big-gunned ships to bomb-laden



aircraft, the Army changed the focus of its defense from coastal forts to anti-aircraft installations around America.

In World War II, advances in missile technology allowed the threat to surpass existing defensive capabilities, and work began on several programs to develop effective missile defense systems. My command is a direct descendent from the Army's Missile Defense Program begun by both Robert Goddard and Wehrner von Braun after the World War II.

After some starts and stops relating to the deployment of antimissile systems designed to defend urban and industrial targets within the United States, President Richard Nixon in 1969 decided to deploy antiballistic missile (ABM) systems only in defense of our intercontinental ballistic missile sites. This was named the Safeguard System, and it called for twelve locations, with construction to begin immediately at two of them—one in Grand Forks, North Dakota, and one at Malmstrom Air Force Base, Montana. Three years later the United States and the Soviet Union signed the Antiballistic Missile Treaty, limiting each nation to only two sites, with one of the locations selected by the signatory and one at each national command center or around the nation's capital.

In 1974, a protocol was added to the treaty, limiting each side to only one ABM site. The system attained full operational capability on September 28, 1975. On February 10, 1976, the Joint Chiefs of Staff, in response to congressional direction, ordered termination of the Safeguard system. Only the early warning radars were exempted from this order.

The Soviet Union installed and has operational today an ABM system around Moscow. The bottom line is that, for 50-plus years after we started developing the ABM system, we have no capability to defend our nation. If you read the vignettes in some of the statements from Representatives from Congress, the general public is either (a) unaware that we have no defense, or (b) thinks that we have a secret plan

that we are not telling everybody about. And neither case is true.

The National Security Strategy and the National Defense Panel clearly indicated the need to prepare the U.S. military to handle the responsibilities of providing defense to the homeland against asymmetrical threats across the spectrum of conflict. Although command and control responsibilities for homeland defense are still under development, National Missile Defense is definitely a contributing element of the larger homeland defense concept. Military assistance to civilian authorities will govern the Army under auspices of the homeland defense mission.

#### The National Missile Defense Program.

There are certain aspects of the Army's National Missile Defense program that directly support the crisis and consequence management efforts of homeland defense operations. They are, to be somewhat specific, assistance in reducing the vulnerability of populations to attack from missiles delivering weapons of mass destruction (WMD); assistance in conducting nuclear, biological, and chemical recovery operations subsequent to missile attack; training of civilian authorities to build confidence in the National Missile Defense system; educating the public on joint and Army national missile defense capabilities; and finally, disseminating missile warning, especially in response to what we see as an expanding threat set.

I want to talk to you about the National Missile Defense program so you'll understand what we are doing. The Department of Defense's (DoD) mission is to develop, demonstrate, and deploy, when directed by the President of the United States, a system to defend the United States against a limited strategic ballistic missile attack. We are very specific when we say that because it is focused on a threat by a rogue nation. Constraints on this mission include the fact that we must be in a position this summer to

support a presidential decision, this system must be developed consistent with the ABM Treaty, and key program decisions are to be phased to reduce risk. You can see that we are working very hard on both the system technology and operational effectiveness. The status of the threat as highlighted in the 1998 Rumsfeld Commission significantly punctuated by the North Korean launch of the *Taepo-dong* missile a month later, and the current national intelligence estimate that I know was alluded to earlier in this conference. The threat is there, and it is growing. System cost is always a concern, and this is not a cheap way of going about our business. And obviously, it is inexorably linked to both on-going arms control negotiations—specifically the ABM Treaty.

These are the key requirements that the Department of Defense under the leadership of the Ballistic Missile Defense Organization are required to account for. In other words, nothing gets through into the United States, the United States being defined as all 50 states. In a highly automated system, we have to have a human in the loop, and, in order to counter the threat, it needs to be a near-real time operation. I am going to go into some depth here so you'll have to bear with me, if you don't mind.

### System Elements.

Let me talk to you about the system elements. The National Missile Defense is a joint Army, Navy, and Air Force system and consists of a number of very complicated aspects. The system includes battle management command, control, and communications elements which are basically the glue that holds everything together. We have upgraded early warning radars that now exist and require some software and hardware modifications and a new ground based radar, which is a radar that does discrimination. We also are planning an arsenal of ground-based interceptors.

The Battle Management Command and Control of the National Missile Defense System will be at Cheyenne

Mountain Operations Center, which is the headquarters for U.S. Space Command and the North American Air Defense Command, where we keep a human in the loop and provide constant communications to the system. In November 1999, the Army was designated as the lead Service for the ground-based portions of the National Missile Defense System. The Army's role is to support the fielding of and then operate the ground-based radars and interceptors and their associated battle management command and control communications. We do this as part of a joint team.

### System Operation.

How does this thing operate? Folks, this is rocket science, and there is no doubt about it. What our folks in government and industry in and out of uniform are doing is truly amazing. Well let's assume a hostile launch to begin the engagement process. (See Figure 1.) That is number 1. A missile is launched at the United States, a space-based sensor makes the initial detection and reports the launch, and that is number 2. The Defense Support Program, and eventually Space Based Infrared System High Component (SBIRS) will alert the entire system of potential ballistic missile attack, cue the radars to erect what we call search fences to detect the incoming missile, and start evaluating the engagement options at the Battle Management Sectors. That is number 3, that big cylinder. When the threat missile crosses into the range of ground-based early warning radars, these radars confirm target missile flight and tracking information. Upon confirmation, the Command and Control Center queues the X Band Radar and directs the launch of the ground-based interceptor. The data will be used by the interceptor to maneuver close enough to the target missile for the on-board Kill Vehicle sensor to discriminate the warheads from the decoys and the debris. I bring your attention to the completely unbiased article in *The Washington Post* on Monday by people who have been saying, for at least 4 decades, that this is an impossible mission. In fact, some of the folks quoted in this article were

quoted in a similar article in the 1976 edition of *Life Magazine* that I have on my desk, which is an interview with Robert McNamara about the system. Well, multiple interceptors launched at each of the incoming reentry vehicles, either in a salvo or waves, are expected to increase dramatically the probability of a successful intercept.



Figure 1. NMD Engagement Concept.

System of Management.

The project manager for this weapons system is the President of the United States. It is not a non-controversial issue. It is replete with defense, political, treaty, funding, technology, and roles and missions concerns. The final decision to deploy or not to deploy the national missile defense capability rests ultimately with the President, in consultation with the Congress of the United States. The present plan calls for a deployment readiness review this July, with a recommendation to the President in late summer or early fall. Should the President make a decision, this is how we think we are going to operate.

The National Missile Defense program as it is currently envisioned will be manned by members of the Army National Guard supported by contract or logistic support. We currently are looking at an organization of about 265 full-time Guard soldiers and about 190 contractors. Of this, we estimate a certain percentage of military and contractors will be located in Alaska or North Dakota, depending upon which deployment location the President approves, with the remainder located in Colorado Springs. We think that the ground-based radar which does the initial discrimination will be located in Shemya, Alaska, in the garden spot of the world out at the far end of the Aleutian Islands. And we are putting the radar there because that is the key place to protect all 50 states. For the missile field we are looking at Fort Greely, and, in fact, I am also on my way to North Dakota the week after next in order to evaluate North Dakota sites.

### System Testing.

We've conducted a number of flight tests of this program. (See Figure 2.) In the top left-hand box, we conducted what we call two integrated flight tests. These were tests to see whether the missile would launch, and the kill vehicle could discriminate targets. No intercept was planned, and both of these tests conducted 2 to 2 1/2 years ago were successful. The next test, the first intercept attempt, is in the upper right-hand corner. That was Integrated Flight Test #3. The purpose of this test was to see if we could launch the missile, get the kill vehicle separated, have the kill vehicle discriminate the warhead from decoys that were launched, and hit the warhead. And that was a very successful test. The test most people have read about is the one on the bottom left-hand corner, which was the partial success but discussed endlessly in the press as a "failure." The kill vehicle missed the re-entry vehicle by 30 meters, but we learned a lot. The next test is scheduled for late June. [Editor's note: That test was conducted as scheduled, and was successful.] This is a launch of a respective threat

missile from Vandenberg Air Force Base, California. If you will envision a tactical ballistic missile launched by a rogue nation toward the United States of America, this is what it would look like in the reverse order of firing from Vandenberg Air Force Base to the Kwajalein Missile Range in the middle of the Pacific, which I run. My operators at Kwajalein and the Battle Management Command and Control monitored the system being used in this test. You can imagine the very sophisticated command and control system that links space-based sensors with ground-based sensors across the world. That is the end of the interceptor vehicle. The entire engagement sequence takes only a few minutes. This is the missile doing its energy management maneuver. Imagine the kill vehicle intercepting a warhead at over 200 kilometers above the earth surface, going in excess of 15,000 miles an hour. The warhead is in a circle because there are other objects that we are asking the kill vehicle to discriminate. Again, this is a crawl, walk, run scenario—an intercept at 15,000 miles an hour, and the warhead was less than five feet long.

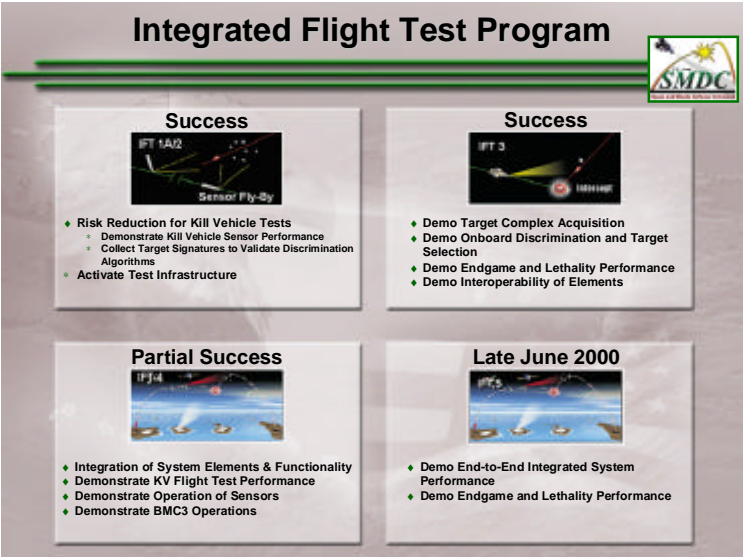


Figure 2. Integrated Flight Test Program.

Because this is one of the most complex systems our country has ever tried to design and develop and because we are on a very tight timeline, the press has not been generous or forgiving. I particularly liked the post-shot rendition from the *Chicago Tribune* that said, "Another in a Series of Failures." Everyone in the program was trying to figure out where the other failures were. Well, we understand the political nature of the beast, and we understand that there are true believers on both sides of this endeavor. It is my purpose today to give you what I feel is a balanced and optimistic approach of what we need to do.

We anticipate the emergence of an increasingly complex threat to the United States both in intercontinental ballistic missiles and cruise missiles, which I have not talked about today. My mission is very clear. My staff and I are doing everything we can to ensure the Army is ready to support the fielding and then the operation of the National Missile Defense system, should the President make a decision to deploy it. And additionally, we are working closely with others to develop concepts and capabilities for the defense of the homeland against the emerging cruise missile threat. (See Figure 3.)

- Full-spectrum missile defense of the homeland will require capability to defeat both ICBMs and CMs.
- The Army is posturing itself to be prepared, when directed, to support the fielding of and then operate its portion of an overall NMD system under the command of USCINCSpace/CINCNORAD.
- The Army is working closely with ASD (C31), USCINCSpace, and other services to develop concepts and capabilities for CMD of the homeland.

Figure 3. Final Thoughts.



This is rocket science. But contrary to what some would have you believe, it is doable. And I am confident from a technological standpoint that we will be able to provide the national decisionmakers with the technological recommendations whereby the president and the Congress can make a decision to deploy or not to deploy this system. Thanks very much.

## CHAPTER 10

### EVOLVING ROLES AND MISSIONS FOR THE RESERVE COMPONENTS IN RESPONDING TO INCIDENTS INVOLVING WEAPONS OF MASS DESTRUCTION

Ellen Embrey

Our nation received a wake-up call with the Oklahoma City, World Trade Center, and Khobar Towers bombing incidents. These seminal events spurred Congress and federal, state, and local government agencies to actively assess the nation's readiness to respond to an incident involving a weapon of mass destruction (WMD). The assessments have led to the development of a plethora of response capabilities, training programs, and research and development initiatives. The federal government has made WMD consequence management (CM) preparedness one of five major program thrusts associated with countering domestic threats, and the President's budget contains \$1.5 billion towards defense against WMD in FY01. Almost 42 percent (\$630M) is dedicated to preparing for and responding to a WMD incident, another 41 percent to research and development, and nearly 13 percent to physical security of government facilities.

Within the \$630M for preparation and response activities, nearly 30 percent is targeted for special response units and between 15-17 percent each for public health infrastructure, first responder equipment, and first responder training and exercising. Combined, the Department of Defense (DoD) has budgeted \$86M in FY01. While seemingly small in relation to the total governmental effort, much of what DoD brings to the integrated response effort is already part of its mission funding, so the above represents targeted funding, specifically for WMD. Of this

amount, the DoD funding profile (\$75M in FY01) is targeted to Reserve Component (RC) integration into this vital area and on which the remainder of this chapter is focused.

Early in the dialog to establish a seamless and integrated response to a WMD incident, the Deputy Secretary of Defense established that Reserve components needed to be fully integrated into the Department's WMD response capabilities.

Why the Guard and Reserve? In part because the Reserve components have always been a forward-deployed force for responding to domestic disasters. So, their participation in WMD incidents was a natural extension of this existing response capability. But more importantly, Guard and Reserve members live and work in more than four thousand communities nationwide and have a unique community-based legitimacy that encompasses regional language and a knowledge of the local geography and urban terrain. They are a part of the community infrastructure and understand the local culture. Many are already familiar with local emergency response plans and procedures and have close links with the fire, police, and emergency medical personnel who will be first on the scene. They may even be an element of the local response infrastructure. Other RC members are already trained in the combat support/combat service support capabilities that are needed in a disaster response situation. Some have experience in performing disaster response with local communities because of a previous response to natural or man-made disasters. For these reasons, our RCs are an obvious first choice for supporting the local responders in almost every situation.

Since 1997, a number of documents have institutionalized RC involvement in WMD CM activities. The "Tiger Team Report," Defense Reform Initiative #25, and two Defense Planning Guidance documents have identified roles and missions and funding responsibilities for the RC. Specifically, the January 1998 Tiger Team Report identified required response capabilities in the

aftermath of a WMD attack and which Reserve components/functions could augment elements of the Federal Response Plan. The Secretary of Defense accepted and implemented some portions of the report through the program budget decision process, which identified resources to ensure the recommendations were implemented.

Also in January 1998, Defense Reform Initiative #25 requested a DoD plan for integrating the Guard and Reserve into domestic WMD terrorism response. Two subsequent Defense Planning Guidance (DPG) documents directed the Services to “program for equipment, operations, exercises, and sustainment of RC response forces that support civil authorities in managing consequences of terrorist use of WMD.” The direction of these two DPG documents was significant because it established WMD CM as a competing priority with other defense initiatives, even though WMD CM response had not been identified as an RC “mission.”

On January 26, 1998, the Deputy Secretary of Defense approved DoD’s Plan for “Integrating the Guard and Reserve into Domestic Weapons of Mass Destruction Terrorism Response.” The approved plan leverages unique Guard and Reserve capabilities to improve DoD’s ability to plan for and respond to the significant and growing threat posed to U.S. citizens by WMD, such as nuclear detonation, release of a biological agents such as anthrax, or chemical substances like sarin gas. Concurrently, it created a new type of unit (WMD Civil Support Team [CST]) to help fill the existing gaps in civilian response capabilities, especially those of local responders, who need to rapidly determine the precise nature of WMD attacks.

The Guard and Reserve share many of the same capabilities, which include aviation operations, search and rescue, engineer operations, transportation, maintenance, law enforcement, fire-fighting, mortuary affairs, explosive

ordnance, bridging operations, communications, command and control, medical assets, and chemical capabilities.

The National Guard has an additional organizational asset unique to the Guard. In many states, the Adjutant General is also responsible for state emergency management. This “dual hat” is often the key to a timely and effective response. Additionally, the Guard, as a state controlled and directed asset, has the ability to get to the disaster event well before other federal assets could respond. Concurrently, the Reserves are part of our federal force and do not report to the governors. Therefore, while they have similar kinds of capabilities, such as airlift and medical forces, as well as unique capabilities, such as Civil Affairs, they are part of the federal response and cannot be engaged until there is a federally declared emergency. This slows the response time but does not diminish their contribution once on the scene. Together, the Guard and Reserve forge a formidable team, already uniquely trained and pre-positioned throughout the United States, ready to respond within hours of a disaster event. Because of these inherent advantages, the DoD is aggressively evaluating how it can leverage existing Guard and Reserve capabilities for a WMD response.

Prior to the initiative to fully integrate the RCs, the Active Components had a variety of response capabilities, most of which were found in the Army: two response task forces, technical escort and explosive ordnance disposal units, defense coordinating officers, and the congressionally-mandated Chemical/biological Rapid Response Team. Additionally, the Marine Corps had a 370-member Chemical-Biological Incident Response Force. Emergency Preparedness Liaison Officers (EPLOs), who are Selected Reserve officers, augmented this WMD response capability. These elements, with the exception of the EPLOs, have a war fighting requirement, but can perform their functions in the United States as part of the regular hazard response for normal disasters, and would be called upon in a WMD incident as well. This assumes a

presidential disaster declaration. But, as was discussed earlier, when time is of the essence, the Guard can be mobilized faster to provide the support that's needed quickly in an initial state response. And key to this initiative was to fully integrate the RCs.

With that goal in mind, some of the capabilities currently in development are primarily state assets. The WMD CSTs (formally known as Rapid Assessment and Initial Detection [RAID] Teams) were designed to be state assets, operating within federal doctrine, but under the command and control of the state governor, via the State Adjutant General; and therefore, they are able to respond to a local/state disaster or emergency well before federal response assets could be brought to bear. Their primary mission is to rapidly respond/move to the incident site to assist the local incident commanders in assessing the nature of the emergency/disaster, to advise local authorities on how to proceed, and to facilitate the application of appropriate DoD support and technical assistance. Ten teams were established in 1999, one in each of the ten Federal Emergency Management Agency (FEMA) Regions. An additional 17 teams have been authorized and will be placed in areas of high population density or in remote areas such as Alaska and Hawaii. FY2000 funding for these teams was \$74.7 million, and the FY 2001 budget request is \$47.9. The existing teams have been undergoing a vigorous training and exercise program, and the final pieces of their equipment are being procured and integrated.

In addition to the CSTs, DoD is also equipping and training existing Guard and Reserve units that already have decontamination and reconnaissance type war-fighting skills on how to work with civilian first responders as part of the incident command system. During the next several years, DoD will complete the training and equipping of over 100 decontamination and nearly 50 reconnaissance elements units in the Army Reserve and Army National Guard. Medical Patient Decontamination Teams in the Air National Guard and Air Force Reserve will

also receive additional training in domestic response casualty decontamination and will be provided with both military and commercial off-the-shelf equipment and enhanced training in civilian HAZMAT procedures.

Finally, the “Tiger Team” report identified 13 additional areas where DoD would most likely be asked to provide support to the civilian community. All are areas where the Guard and Reserve maintain considerable mission capability and are areas we are going to explore in more depth. These include support in five medical areas: stress management, NBC medical response, medical decontamination, preventive medicine, and pharmacology. In the next few years, DoD will also examine leveraging existing Guard and Reserve capabilities in communications, transportation, logistics, mortuary affairs, information, security, and engineering.

While we can point to notable successes in establishing and integrating our RCs into the WMD response, there are still significant challenges to overcome before we reach full integration. The stand-up of the Joint Task Force Civil Support at United States Joint Forces Command will provide an on-scene standing military organization structure and command and control capability. The recently published RC Employment-2005 Study identified several WMD CM roles for the RC, but also pointed out that there is a severe shortage of force protection equipment for our forces, both active and reserve, which may limit their ability to effectively respond. This is an area that must be addressed quickly. Finally, it is likely that any WMD incident will require a regional response rather than a local or state effort. Effecting this response will require better coordination and organizational integration, and additional training and exercising, if we are to be successful.

Security is a national imperative. DoD is taking comprehensive steps to execute policies and plans to better prepare and respond to an ever increasing array of threats, including the domestic use of WMD. DoD will continue to

explore ways to make our RCs a fully integrated part of our national WMD threat response.



# CHAPTER 11

## IN SUPPORT OF THE CIVIL AUTHORITIES

Donald A. Haus

Military assistance to civilian authorities is not a new concept. From before the birth of this nation, the military, whether militia or regular or both, has habitually supported local, state, and federal civilian authorities in times of manmade or natural disaster, civil unrest, or other situations. This support was very often questionable in legality and usefulness. Over time, though, numerous laws and directives have transformed this supporting relationship into an institutionalized interdepartmental and interagency coordination and planning process. The changing nature of threats, however, has expanded the scope of the military's responsibilities in support of civilian authorities. This old mission now involves an ever-widening array of diverse military and Department of Defense (DoD) organizations and agencies equipped with new terminology and new, evolving concepts.

The United States faces myriad threats today besides those caused by natural phenomenon. Many factors make these threats more ominous. Foremost is U.S. preeminence as a world power. Groups opposed to the thrust of our post-Cold war policies have multiplied in recent years. The openness of the U.S. society provides an opportunity for our enemies to operate with more freedom than they would have in more restrictive venues. Also exacerbating the threats is the global proliferation of cheap Weapons of Mass Destruction (WMD). These threats can be described as either international or domestic. International threats fall into one of three separate categories: international terrorism, transnational threats, and conventional attacks. The first category, international terrorism, consists of nations who view terrorism as a tool

of foreign policy such as Iran, Iraq, Syria, Libya, Cuba, and North Korea, autonomous, transnational terrorist organizations or groups possessing their own infrastructures, personnel, financial arrangements, and training facilities, and, finally, the loosely affiliated extremist groups. The reasons for any type of terrorist attack by these groups are as varied as the groups or the individuals themselves. They range among revenge, publicity, political change, visibility, financial gain, and chaos!

Transnational threats are comprised of any transnational activity threatening the national security of the United States. This includes international terrorism, narcotics trafficking, the proliferation of WMD and the delivery systems for such weapons, and organized crime or any individual or group that engages in such activity.

The U.S. homeland appears to be impervious to conventional attacks, as we know them in the foreseeable future. Nevertheless, the possibility of such attacks exists, especially an aerial or maritime attack using conventional platforms.

Domestic terrorism stems from domestic groups who are based and operate entirely within the United States, its territories, or possessions, and whose activities are directed at elements of the federal, local, or state governments or the U.S. civilian population. The United States is experiencing a rapid growth in domestic terrorist groups.

The Critical Foundations Report of the Presidential Commission on Critical Infrastructure Protection asked how the United States could protect itself from any terrorist threat. A simple but realistic answer is that the best protection besides vigilance is preparation. Being prepared is the responsibility of every citizen, community, business and government. For those in DoD, it is even more critical because its responsibilities are spread over a large arena.

Figure 1 entitled “Homeland Security” provides an excellent look at this diverse arena. Homeland Security (formally known as Homeland Defense and still not an approved term) is defined as protecting our territory, population, and critical infrastructure at home by:

- Deterring and defending against foreign and domestic threats.
- Supporting civil authorities for crisis and consequence management.
- Helping to ensure the availability, integrity, survivability, and adequacy of critical national assets.

Homeland Security has a full line-up of players. Not only do we have the mission spread between several Unified and Functional Commands, but these commands must act in support of a number of Lead Federal Agencies (LFA). The areas of responsibility of these Federal Agencies often overlap with the result that DoD may find itself supporting several federal agencies simultaneously.

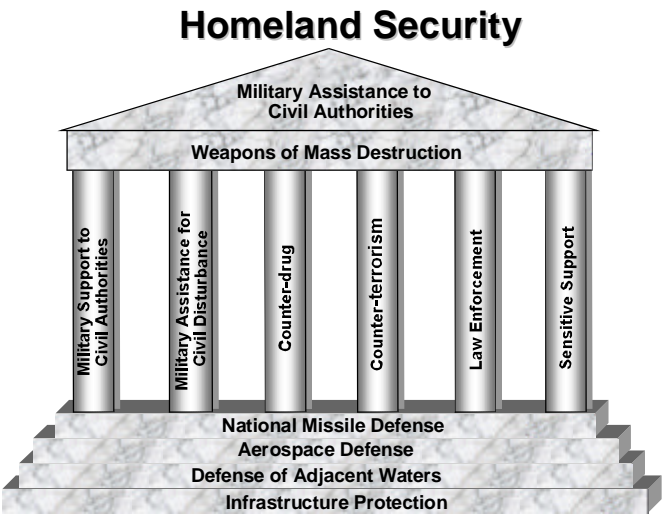


Figure 1.

A possible example of this is a domestic WMD incident. The FBI has the lead in crisis management for the incident whereas the Federal Emergency Management Agency (FEMA) would have the lead for consequence management operations. However, the FBI retains overall the role as LFA until they release it to FEMA. Even with all this federal support, the local and state responders will be the first on the scene and will usually remain in charge to coordinate consequence management operations. *Our challenge in this is to try to integrate and coordinate an effective DoD response to support civilian authorities. This is accomplished by thorough planning.*

Under the Constitution, the civilian government is responsible for preserving public order and carrying out governmental operations within its territorial limits. The DoD may provide forces to support civil authorities to mitigate the effects of civil emergencies—catastrophic fires, hurricanes, floods, civil disturbances, and earthquakes. Such support usually occurs after a presidential declaration of a major disaster or an emergency. The support is designed to supplement the efforts and resources of state and local governments and voluntary organizations but only for a limited time and until the civil authorities can reasonably accomplish these tasks without DoD support. The Federal Response Plan (FRP) provides the national architecture to coordinate the actions of all supporting federal agencies including DoD.

Army forces will provide support as part of the DoD effort primarily in accordance with DoD Directive 3025.15, Military Assistance to Civil Authorities (MACA). The MACA directive is wide ranging and address both natural and man made disasters and includes military assistance to civil disturbances, counterdrug activities, combating terrorism, and law enforcement. The Secretary of the Army is designated as the DoD Executive Agent for non-WMD MACA. (See Figure 2.)

```

graph TD
    President[President] --> LeadFederalAgency[Lead Federal Agency]
    President --> SecDef[Secretary of Defense  
Secretary of the Army]
    SecDef --> JOINTSTAFF[JOINT STAFF]
    SecDef --> DOMS[DOMS  
Deputy DOMS]
    SecDef --> USJFCOM[USJFCOM (CONUS)]
    SecDef --> USSOUTHCOM[USSOUTHCOM (P.R./U.S.V.I.)]
    SecDef --> FORSCOM[FORSCOM]
    SecDef --> USPACOM[USPACOM (Pacific/Alaska)]
    SecDef -.-> ActionAgent[Action Agent]
    SecDef -.-> OperatingAgent[Operating Agent]
    SecDef -.-> LOA[LOA]
    LeadFederalAgency -.-> Coordination[COORDINATION]
    JOINTSTAFF -.-> Coordination
    DOMS -.-> Coordination
    USJFCOM -.-> Coordination
    USSOUTHCOM -.-> Coordination
    FORSCOM -.-> Coordination
    USPACOM -.-> Coordination
  
```

The diagram illustrates the organizational structure of the Department of Defense. At the top is the President, who oversees the Lead Federal Agency and the Secretary of Defense (who also serves as the Secretary of the Army). The Secretary of Defense oversees the JOINT STAFF, DOMS (Deputy DOMS), and five major military commands: USPACOM (Pacific/Alaska), USJFCOM (CONUS), USSOUTHCOM (P.R./U.S.V.I.), FORSCOM, and another command (partially obscured). The diagram also shows three types of agents: Executive Agent (Secretary of Defense), Action Agent (DOMS), and Operating Agent (USSOUTHCOM). A COORDINATION line connects the Lead Federal Agency, JOINT STAFF, DOMS, and all five military commands. A LOA (Line of Authority) is shown for FORSCOM.

Figure 2.

The Secretary of the Army uses the Director of Military Support (DOMS) as the Action Agent to plan, coordinate, and direct MACA operations across all Commander-in-Chief (CINC) lines. The military services and DoD agencies all lend support to the effort. In the case of MACA, there are three CINCs who have the responsibility for all U.S. territory as follows:

- United States Joint Forces Command (USJFCOM) — 48 contiguous states;
- United States Pacific Command (USPACOM) — Alaska, Hawaii, and the Pacific Islands;
- United States Southern Command (USSOUTHCOM) — Puerto Rico and the U.S. Virgin Islands.

The DoD uses a standard organization within the CINCs to execute MACA mission. Figure 2 shows a basic template of the DoD Support to an incident. Each CINC is responsible for planning and executing MACA operations in his area of

responsibility. Two of the CINCs use a subordinate command to execute the mission. Within USJFCOM, Forces Command is the subordinate command appointed as the Lead Operational Authority (LOA) for planning and executing non-WMD MACA.

Forces Command has a broad range of domestic support responsibilities as USJFCOM's Lead Operational Authority for Military Support to Civil Authorities. Forces Command's most challenging responsibilities are to develop USJFCOM domestic emergency plans, coordinate with FEMA for disaster response IAW the Federal Response Plan, train DoD Defense Coordinating Officers (DCO), monitor the readiness of specialized Reserve Component WMD response elements, and execute military operations in support of many emergency activities. As the Army component for USJFCOM, FORSCOM also provides units, equipment, and other resources for MACA missions as directed by CINCUSJFCOM.

The Commanding General, FORSCOM, currently conducts regional disaster relief planning, coordination and execution through the two Continental U.S. Army's (CONUSA): the First United States Army located at Fort Gillem, Georgia, and the Fifth United States Army located at Fort Sam Houston, Texas. The First U.S. Army oversees 27 states and the District of Columbia that comprise FEMA Regions I, II, III, IV, and V. The Fifth U.S. Army area of responsibility consists of 21 states and encompasses FEMA Regions VI, VII, VIII, IX, and X.

For certain type of missions, usually natural disasters, requiring limited DoD support, a CINC will dispatch a Defense Coordinating Officer (DCO) to serve as the DoD single point of contact for providing DoD resources. The DCO validates mission requests from a civilian Federal Coordinating Officer (FCO) located at the local FEMA federal disaster field office and coordinates the appropriate military response.

## Army Regional Planning Agents

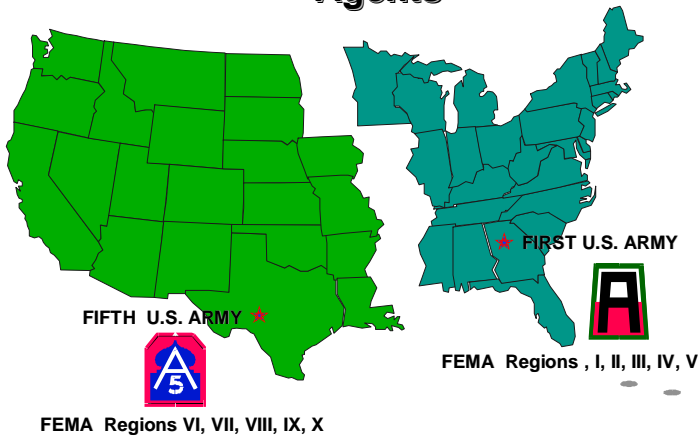


Figure 3.

The DCO is an active duty position. By DoD Directive, the appointed DCO will be a military officer in the grade of O-6. The DCO is not always an Army officer. However, the Army (Forces Command) has pre-designated and trained a cadre of Army colonels to specifically perform this function. Each of FORSCOM's Training Support Brigade (TSB) Commanders and Colonel Senior Army Advisors are trained to be a DCO and assigned to a particular state.

The DCO will coordinate disaster requests for assistance with the CONUSA. The CONUSA may then supply the requested asset or ask for FORSCOM to source the request. The DCO maintains Operational Control (OPCON) of all assigned DoD Forces, except the United States Army Corps of Engineers (USACE), operating in the disaster area. Also, the National Guard of each state is committed under State Active Duty and will not be OPCON to the DCO. The Guard remains under state control during disaster relief.

During very large disasters, a Joint Task Force (JTF) may be created for C2. In these cases, the DCO maintains

the same relationship with the FCO. The DCO accepts the taskings from the FCO and passes these to the JTF for execution. Additionally, now the JTF maintains OPCON of all DoD assigned forces in the disaster area (except U.S. Army Corps of Engineer assets).

Within DoD, each service maintains a cadre of specifically trained reserve officers assigned to coordinate MACA missions in each FEMA region and each state. These positions are drilling reserve officers, not Active Guard or Reserve (AGR) or active duty. As a condition of employment, each Emergency Planning Liaison Officer (EPLO) agrees to volunteer time during a disaster. Once voluntarily activated, the EPLOs work in support of the FEMA region or the appointed DCO for the disaster. The EPLO's role is to help liaison and coordinate between the FEMA, state, and local officials and DoD. EPLOs are expected to become experts on the plans and procedures within their respective federal region and state. State EPLOs are also expected to become familiar with all service capabilities within their state and establish relationships with service installation commanders. Even though the EPLOs are not commanders nor do they control assets, they are the eyes and ears of the RPA and DCO. The EPLOs are assigned within the 10 FEMA regions and in each state, territory or commonwealth. They are also located many different military organizations: at the two CONUSAs, FORSCOM, the Air Force National Security Emergency Preparedness (AFNSEP) headquarters, the Air Force Emergency Headquarters Relocation Site, the Director of Military Support, and the Office of the Deputy Under Secretary of Defense for Preparedness.

The WMD Act of 1996 directed DoD to organize a response task force (RTF) for WMD incidents. DoD subsequently formed two RTFs: RTF-East located in the First U.S. Army area and RTF-West located in the Fifth U.S. Army area. The RTFs are separate and distinct from JTFs used for disaster relief missions and are specified for deployment to WMD incidents only. The RTF would be



OPCON to USJFCOM during support to crisis management and upon direction of the CINCUSJFCOM, may revert to OPCON to the FORSCOM Commander during support for consequence management.

The RTF commander, usually a CONUSA Deputy Commanding General, forms the organization using internal personnel and equipment resources of the CONUSA headquarters. FORSCOM allocates Army active duty and Army Reserve units based on mission requirements and the task force continually grows or shrinks as mission requirements change.

Today, the RTF commander, also has a limited number of specially focused response assets to call upon for WMD incidents. These elements, including the Army's Technical Escort Unit (TEU), the Navy's Medical Research Institute Lab, and the Marine Corps' Chemical Biological Incident Response Force, are specially trained and equipped to respond in a nuclear, biological or chemical environment.

A 1999 DoD Directive further expanded the military's ability to respond to a WMD incident. This directive named the USCINCFJFCOM as the Executive Agent for WMD consequence management in the Department of Defense. USJFCOM has primary responsibility for planning and executing MACA for consequence management for WMD incidents within the United States, its territories, and its possessions. Its primary focus is developing, coordinating, reviewing, and maintaining all Joint Doctrine and Joint Tactics, Techniques and Procedures (JTTP) to guide services in executing consequence management operations. USJFCOM was also tasked to create a standing Joint Task Force for Civil Support (JTF-CS). The JTF-CS is a deployable headquarters created to plan, coordinate and execute DoD support for domestic WMD incidents. The operating concepts and procedures for this newly formed organization are still being solidified.

The military must continue to improve upon existing readiness and develop the capabilities, technologies, and

techniques that will be required to confront any form of attack on the U.S. homeland. The Army, as a member of the joint team, must be ready to respond and support the civil authorities of this country against any disaster, incident or attack no matter what shape or form it comes in. The country demands our knowledge, our expertise, and our courage. When we look in the eyes of the American public we must be able to honestly say—"We did our best."

## CHAPTER 12

### WHERE DOMESTIC SECURITY AND CIVIL LIBERTIES COLLIDE<sup>1</sup>

Charles J. Dunlap, Jr.

Imagine, if you will, that there was fairly hard evidence that next year a group of people would kill 40,000 Americans, injure another 6 million,<sup>2</sup> and inflict some \$150 billion in economic losses on this country.<sup>3</sup> Compare that situation with a problem that last year killed or injured no one and cost, at most, some \$8 billion.<sup>4</sup> Which one would—or should—garner the most attention of the national security community?

One would think that the military would put emphasis on the former, while the latter would be left to state or federal law enforcement personnel to sort out. Actually, the focus is much the reverse. The first set of numbers describes the annual impact of motor vehicle accidents while the second represents the combined costs of nuclear, biological, chemical, and cyber attacks on the United States. Still, some experts—many of whom once apocalyptically touted Y2K<sup>5</sup> perils—insist that the U.S. homeland is exceptionally vulnerable to such threats. And the U.S. military is listening. Today, it is beginning to pour resources into efforts to defend against dangers that have rarely manifested themselves not only here, but *anywhere*.

It is, of course, true that the *potential* dangers posed by weapons of mass destruction (WMD) are very great—in theory. No one disputes that we should take prudent steps to defend against them. Prudence dictates, however, a hardnosed assessment of risk so that reasonable decisions are made as to how to focus effort and allocate scarce resources. Accordingly, as we look at the many challenges facing the armed forces today, we ought to consider that during the period 1993-98 (the latest government figures

available) there were only seven casualties (primarily as a result of the World Trade Center bombing) from *any* international terrorist action in North America.<sup>6</sup>

Nevertheless, the U.S. Government has stepped up its efforts to combat terrorism. For example, Presidential Decision Directive 62 (PDD-62) was issued in 1998. PDD-62 made fighting terrorism “a top national security objective” to be pursued with the “goal of ensuring that we meet the threat of terrorism in the 21st century with the same rigor that we have met military threats in this century.”<sup>7</sup> Despite the rhetoric of a “national security objective,” terrorism remains formally a law enforcement problem, and our official aim is to “bring terrorists to justice for their crimes.”<sup>8</sup> Law enforcement problems are, of course, not a traditional responsibility of the uniformed services.

Clearly, not every threat to “national security” is by definition the responsibility of the armed forces. Failing schools, economic troubles, and social unrest may all imperil national security broadly construed, but it does not necessarily follow that the military should provide solutions. The courts have repeatedly held that the purpose of the armed forces is “to fight or be ready to fight wars should the occasion arise.”<sup>9</sup> Yet the military is ever more frequently employed to confront a broader range of national ills. Why? One reason is that the military seems to get things done. In a very insightful 1991 article in *Atlantic Monthly* magazine, James Fallows wrote, “I am beginning to think that the only way the national government can get anything worthwhile done is to invent a security threat and turn the job over to the military.”<sup>10</sup>

In my view, when what is “turned over to the military” is something that is principally a law enforcement problem, the military—and the nation—assumes risk. There are relatively few modern examples where systematic use of the military to meet internal security threats has been good for democracy or, for that matter, the military itself. As to the latter, consider the performance of the Argentine Army

during the 1982 Falklands/Malvinas conflict. Argentine soldiers, who had proven themselves rather expert at torturing and killing their fellow citizens in internal security operations, were rather less effective when facing the British Army on the battlefield. The mere presence of *real* soldiers—the Gurkha Regiment and elite paratroop units—panicked many Argentine conscripts into surrender with hardly a shot fired. Internal security duties do something to military forces, and I submit it is not something good for warfighting.

But let us focus on the impact on democratic values of the regularized use of the military for policing-type duties. I believe the Founding Fathers would be rather horrified at the suggestion that the regular military forces, the “standing army” so to speak, were to be used in any systemized way for internal security. They were very cognizant of the excesses of Cromwell’s New Model Army in England,<sup>11</sup> and resented the use of Royal troops in the colonies to suppress the growing protest against imperial rule.<sup>12</sup> The killing of five colonists in 1770 by the British Army still resonates as the “Boston Massacre.”

From the very beginning, Americans considered a standing army a threat to liberty. They also did not like supporting troops through taxes or otherwise. In fact, the infusion of British regulars into local communities was the reason one of the least known parts of the Constitution, the Third Amendment, was later adopted. This provision—which sounds quaint to modern ears—forbids the quartering of troops in private homes without the consent of the owners. We are hardly aware of this Amendment because the military establishment has wisely avoided doing things that would awaken latent antimilitarism infringing upon Americans in their home.

To me, history teaches us that there is a form of antimilitarism deeply embedded in the American character.<sup>13</sup> It is usually benign, but represents a potential that today’s militaries must never forget. We should keep in

mind that what the architects of the Constitution really hoped was that a professional military of any size would not be required.<sup>14</sup> In terms of a military establishment, they conceived of one not designed for force projection but rather an organization distinctly defensive in character. It would center on a small cadre of full-time professionals who would be augmented in wartime by mustering of huge state militias. The militia system never really worked as originally envisioned, but, up until the start of the Cold War, the pattern in the United States was a small standing peacetime force that grew rapidly during conflicts through the massive addition of volunteers and conscripts.

The small size of the professional military, if nothing else, precluded much interference with the rights of American citizens during most of U.S. history. Wartime did create exceptions, but Americans generally did not like the experience. During the Civil War, for example, the military sought to exercise martial law authority.<sup>15</sup> In the case of *Ex Parte Milligan*,<sup>16</sup> a civilian—a lawyer, incidentally,—was tried by military commission for various seditious acts and sentenced to death. The Supreme Court ultimately threw out the conviction, holding that, so long as the civil courts remained open, the military could not extend its authority to civilians, even under the exigencies of national security in wartime.

One of the principal examples of the *systemized* use of the armed forces for law enforcement in peacetime was in the post-Civil War south. Again, the experience was not a good one and eventually produced legislation that today represents the principal legal impediment to the use of the military for law enforcement duties. Largely as a result of questionable activities of federal troops in response to a railroad strike and during the election of 1878,<sup>17</sup> Congress passed the Posse Comitatus Act.<sup>18</sup> That statute—which was welcomed by most military officers at the time<sup>19</sup>—criminalizes the use of the armed forces to execute the laws (subject to a few exceptions). As influential as it is

in many situations, there has never been a conviction for violation of the Act.

Of course, troops have always been used to suppress riots and other domestic civil disorders throughout U.S. history.<sup>20</sup> These were mainly situations where the disturbances plainly exceeded available police resources. Perhaps the darkest, most disturbing uses of the military for internal security purposes was during the 1960s and 70s, a period made turbulent by the confluence of civil rights and antiwar protests. Professor Loch Johnson reports that, not only was the National Security Agency secretly recording every cable sent overseas by Americans for almost 30 years, "Army intelligence units conducted investigations against 100,000 Americans during the Vietnam War."<sup>21</sup> A Senate investigation (the Church Committee) in the early 1970s made public for the first time the extensive scope of the military's surveillance of U.S. citizens.<sup>22</sup> When the military's activities were revealed, a plethora of legislation and other regulations followed.<sup>23</sup> These still limit the information the armed forces can collect on American citizens domestically. So damaging were the excesses exposed, the military's appetite for domestic security activities dampened markedly.

By the early 1980s, however, the drug crisis in this country catalyzed Congress into passing a number of legislative initiatives to involve the armed forces in the war on drugs.<sup>24</sup> The United States was in the midst of a crime wave for which illegal narcotics was much to blame, and which Congress believed was overwhelming police forces. The new authorities still restricted the military from engaging in direct law enforcement activities, such as search and seizure, and arrests—but they did permit the provision of training, equipment, and specialized technical services. The nearly 2-decade effort has cost billions and involves even today thousands of soldiers, sailors, and airmen. As will be discussed below, these activities can be controversial.

Today, we see fears of terrorism against homeland targets fueling a renewed effort to involve the military in domestic security. This is especially true with respect to cyberterrorism. In May of 1998 Presidential Decision Directive (PDD) 63<sup>25</sup> was issued which sets out a blueprint to expand the role of the Department of Defense (DoD) in countering cyber terrorism. Specifically, DoD is listed as the "lead agency" in the area of "national defense."<sup>26</sup> As such, DoD is "coordinating all of the activities of the United States Government in that area."<sup>27</sup> PDD 63 does not, however, define the parameters of "national defense,"<sup>28</sup> an especially problematic situation given the dual-use (i.e., used by both military and civilian persons) nature of many of the systems subject to cyber assaults. How can DoD escape intruding into civilian areas with such a loosely defined mission?

Other steps also have been taken just in the last year or so. Notwithstanding the withering criticism of the National Security Agency (NSA) by the Church Committee in the 1970s, DoD has assumed an "information assurance mission."<sup>29</sup> According to its own public documents, it "conducts defensive information operations, to achieve information assurance for information infrastructures critical to U.S. national security interests."<sup>30</sup> Towards the end of 1998, DoD also established Joint Task Force Computer Network Defense (JTF-CND)<sup>31</sup> and tasked it to coordinate the defense of all DoD computer systems.<sup>32</sup> In October 1999 JTF-CND,<sup>33</sup> along with the Joint Information Operations Center was placed under the control of U.S. Space Command (USSPACECOM). In a separate project, DoD established the Defense Computer Forensics Lab in September of 1999.<sup>34</sup> Among other things, the lab seeks to chase across the Internet hackers who assault DoD systems.<sup>35</sup>

Not all of the recent effort has focused exclusively on defending against domestic cyber attacks. After discussion of the establishment of a "Homeland Defense" command was aborted when civil libertarians complained, DoD established Joint Task Force-Civil Support (JTF-CS).



JTF-CS has a relatively uncontentious charter that merely tasks it to assist civilian authorities in “consequence management,” that is, dealing with the after effects of a catastrophe, regardless of its source, but most likely the result of terrorism involving WMD, including cyberterrorism. In announcing the new task force, DoD conceded that the benign title of “civil support” and the selection of a National Guardsman instead of a Regular officer as the commander were both intended to quell the concerns of civil libertarians who feared that the “DoD was out to take over and would trample people’s civil liberties” with the new organization.<sup>36</sup>

Parenthetically, it seems to make sense that many of these homeland defense missions would default to the National Guard. Conceptually, such a mission would appear to fit with the traditional, local orientation of the Guard. Moreover, its historical citizen-soldier model should temper public concerns about an overreaching “standing army.” In a way, however, Total Force has been too successful. With fewer and fewer members of the public showing any military experience in their resumes, the average citizen perceives no differences among those persons in uniform. Everyone—regardless of component—is, for example, “the Army” in a corporate sense to the proverbial “man in the street.”

Accordingly, any improper action by one component will probably be imputed to all. Another Kent State shooting will undermine the reputation of the Regular Army, notwithstanding that the Reserves or Guard might have committed the act. Thus, it is unlikely that designating a Guard officer as the JTF-CS commander as opposed to an officer from another component will have any real ameliorating effect on potential civil-military relations friction. It may even have an aggravating effect because the Guard (and to a lesser extent the Reserves) has no tradition of being apolitical. The openly political behavior of some in the Guard carries great potential to create tensions between

the armed forces and the citizenry if the trend towards greater involvement in law enforcement activities persists.

Why is the use of armed forces as an internal security tool considered so suspect by civil libertarians and others? Secretary of Defense William Cohen captured a key issue, when speaking about the frustrations of the Army's attempts to police areas in Kosovo, commented in January 2000 that the Army is "not trained for that; they are not competent really to carry out police work, nor should they be doing it."<sup>37</sup> Cohen is right, but not just in the Kosovo context. From the constabulary peacekeeping missions of the 1990s, we learned that the skills of the combat soldier are not necessarily coterminous with those of the policeman.

Although this should be intuitive, many uniformed people fail to sufficiently appreciate that there are fundamental differences and, I would submit, *incompatibilities* between the *culture* of the soldier and culture of the policeman. One could almost say that the mental wiring is different. For example, it always amazes me that some officers believe that their oath to "support and defend" the Constitution against "all enemies, foreign and domestic"<sup>38</sup> is somehow license (if not duty) to engage in domestic law enforcement activities. It is as if they believe that persons suspected of crimes are somehow domestic "enemies" of the state. Of course, under our system of law, those accused of crimes are *innocent* persons until proven otherwise in a court of law—not enemies of the state, domestic or otherwise. But military people are oriented to think of adversaries as enemies, not as suspects entitled to the presumption of innocence.

This difference in thought patterns manifests itself in other ways as well. Members of the armed forces think of power in brute, physical terms: mass, weight of effort, rates of fire, and so forth. A law enforcement officer draws his power not from his weaponry *per se*, but from moral authority his status and position in society exerts. It is interesting to note that experts are starting to realize that

the militarization of the police in the past two decades, that is, their tendency to ape military organizations through SWAT units, heavier weapons, body armor, and so forth, may well be counterproductive. Such factors undermine their effectiveness by creating a new mindset based on *physical* power that diminishes their moral authority. In discussing the explosion in the number of disturbing incidents across the country of heavy-handed police behavior, former police chief John McNamara admitted recently that “some corrosive assumptions [have] crept into police culture.”<sup>39</sup> He says,

The fundamental duty of police is to protect human life. But in many places that understanding has been superseded by a militaristic approach, one that allows for an acceptable number of casualties and that views much of the population as hostile.<sup>40</sup>

Military authorities ought to take note of the problems that a “militaristic approach” generates. Moreover, just as some in the armed forces tend to perceive American citizens suspected of crimes as “enemies” of the state, military members can also evaluate threats very differently than do properly-focused and trained law enforcement personnel. Consider the 1997 shooting of a Texas teenage shepherd by a Marine Corps border surveillance patrol. The youngster (who was probably unaware of the camouflaged military presence) may simply have been casually shooting at game as he tended his flock, but the Marines seem to have mistook this as fire being directed against them, and responded with deadly force. A policeman faced with a threat may well retreat and contain a situation out of concern not only for himself and other innocents, but also for the safety of the “threat” itself. But a military person thinks of destroying threats, not keeping them safe for arrest and judicial disposition, and this may have been a factor in the Texas shooting.

Consider this mindset in the cyberterrorism context. If you do, it should be no surprise—given the military’s

perspective—that a Pentagon-sponsored report argued that the Pentagon’s “policy of prohibiting DoD from mounting a counter cyberattack if its computers are attacked puts the military at risk.”<sup>41</sup> In responding to the report’s proposal to allow the military to immediately launch an electronic counterattack, John Pike of the Federation of American Scientists quipped, “Does this mean that the Pentagon will start frying the home PCs of American teen-age hackers?”<sup>42</sup> I hope not, but maybe.

Furthermore, the threat of cyberterrorism is generating calls from some to abandon the policy that limits the use of the military’s intelligence gathering and other resources against domestic cyber-incidents. U.S. policy today assumes that, absent evidence to the contrary, cyber assaults involve U.S. persons. The presumption of a “U.S. person” means that it is thus first and foremost a law enforcement matter. This ensures that the judicial process is used in the event intrusion into the citizenry is required in the course of the investigation. It also greatly limits the involvement of the military, and especially its intelligence gathering assets. The new proposals call for a revised policy that presumes the digital “intruder is *not* a U.S. person,” thus permitting “the full capabilities of the United States’ investigative and intelligence assets” to be “brought to bear” as some desire.<sup>43</sup> Legislation allowing the military and other intelligence agencies to investigate U.S. citizens is currently under consideration.

I believe such proposals are often welcomed within the military establishment (and even outside of it) because it is not well appreciated exactly why the armed forces represents a far greater threat to civil liberties than do even the most robust law enforcement organizations. The genius of the American scheme of law enforcement organization from a civil liberties perspective is that the power represented by more than 780,000 sworn officers is diffused into over 18,000 independent or semi-independent police forces subject to local control. If a particular agency runs amok, there is ample counterbalance available. There is

really no similar counterbalance to the U.S. military establishment. This is not much of a concern so long as the armed forces remains *externally* focused—the threat to rights at home is minimized. But no such assurance can be made once the physical power, mental energy, and organizational unity of the armed forces turns inward toward the American citizenry itself.

Nevertheless, the military *must* turn inward *if* the threat to homeland security is such that existing law enforcement agencies are incapable of dealing with it. We must recognize that if that occurs, civil liberties are almost certain to be at risk. In 1997 Secretary of Defense Cohen admitted,

terrorism is escalating to the point that citizens of the United States may soon have to choose between civil liberties and more intrusive forms of protection.<sup>44</sup>

The “more intrusive form of protection” could, of course, involve the military.

The armed forces certainly have a role to play in confronting terrorism, but not necessarily an intrusive one. In the short term, I believe that the military’s role in consequence management is a necessary one—there really is no option in the case of a cataclysmic nuclear, biological, or chemical attack. While it may be wise to build and equip the necessary consequence management organizations in the civilian sector as is currently underway, it seems to me that the episodic nature of such events, as well as the limited scope of the military’s role, makes the risk to civil liberties manageable.

I am much more concerned about the use of the military to confront the threat of cyberterrorism. The invasive nature of cyber investigations, as well as the technical difficulty of determining the origin of cyber attacks, almost by definition will result in military confrontations with U.S. citizens, many of whom will be innocent of any offense. The key question is whether or not military involvement is

really warranted by the threat. In my view, it is not. I believe that all the dour predictions that a teenager with a Palm Pilot could hack New York into darkness are wildly overblown.

Writing in the winter issue of *Foreign Policy*,<sup>45</sup> cyberwar expert Martin Libicki asserts that conducting a truly meaningful attack on critical computer systems is far more difficult than popular wisdom suggests. Libicki points out that if it were really as cheap and as easy to do as so many cyberzealots claim, someone, somewhere, would have done it already. Countering this view, Professor Dan Kuehl of the National Defense University testified before Congress in February on this issue. He said that the reason a full-fledged cyberattack has not been launched is "solely because no state or non-nation state actor has yet seen sufficient strategic advantage to be gained by doing so—and this condition will not last indefinitely."<sup>46</sup>

I do not share Professor Kuehl's view. There are too many actors out there—Slobodan Milosevic, Saddam Hussein, Osama bin Laden, and many others—who would surely hurt the United States *if they could*, especially if they could do so anonymously as the cyberzealots insist is possible. Looking beyond our borders, does anyone seriously believe that Chechens would refrain from launching a devastating computer attack against Russia? Would they see no "strategic advantage" in doing so, even though their country is being demolished and their people slaughtered by Russian troops? What about the Kurds suffering in Iraq? Or Turkey? How about the IRA against Britain?

The idea that *all* of these different groups would come to precisely the same strategic conclusion to "desist" *vis-à-vis all* these potential targets despite profound cultural differences simply strains credibility too far. The real reason crippling attacks have not taken place is that it is just too hard to do—and getting harder every day as the financial rewards of e-commerce are stimulating vast expenditures for net security. Keep in mind that I am not

talking about denial-of-service attacks<sup>47</sup> that close down a commercial web site for a couple of hours<sup>48</sup>—that should not be a military concern—I'm talking about taking down the nation's critical infrastructures for a significant period.

Does this mean that serious and costly cyber incidents will *never* occur? No. It merely means that there is insufficient evidence today to require a *military* role in the law enforcement aspects. Even a hugely tragic incident involving thousands of deaths and billions in damage are no more of a risk—and no more beyond the abilities of traditional law enforcement entities to address—than are, as previously discussed, the motor vehicle accidents we suffer every year or, for that matter, the World Trade Center or Oklahoma City bombings. We should recall that Martin Van Creveld maintains terrorism has not succeeded in developed states because modernity itself produces redundancies and work-arounds that rapidly mitigate even savage attacks.<sup>49</sup> Cyberterrorism cannot bring America to its knees.

The military ought to get involved in homeland cyberdefense when it becomes apparent that some opponent has a genuine capability to inflict losses extensive enough to truly *cripple* critical military or civilian systems in such a way as to really harm to our vital interests and threaten our way of life. I do not believe such proof exists. Nevertheless, our military and civilian leaders repeatedly insist we are vulnerable to an “electronic Pearl Harbor.”<sup>50</sup> Using the rhetoric of the infamous sneak attack is a clever way to shock people into supporting the kind of civil liberty compromises about which Secretary Cohen spoke.

To me, however, Pearl Harbor suggests other images. They are scenes of U.S. Army troops herding loyal citizens into barb-wired detention camps because of rhetoric about a threat that in reality was nonexistent. Although it may be fashionable today to say that racism explains the treatment of Japanese-Americans in the wake of Pearl Harbor, the reality is much different. A careful reading of the Supreme

Court's decision in *Korematsu v. United States*,<sup>51</sup> reveals that honorable men in the embrace of genuine—albeit wildly mistaken—fears made the decision to incarcerate hundreds of thousands of equally honorable American citizens. That said, we should learn from this history the *real* danger to American values posed by overestimation of the dangers we face.

As we calculate the risks of an enhanced role for the military in homeland defense, we should recall that the damaging revelations of the Church Committee in the early 1970s heralded a post-Vietnam downward slide for the Army and the military in general. After an enormous effort in the late 1970s and 1980s, the U.S. armed forces emerged to become what is today the most trusted institution in American society.<sup>52</sup> Yet we seem to have forgotten the lessons of the past. I am absolutely convinced that a deepening involvement of the armed forces in any kind of domestic activity associated with law enforcement or investigations carries great potential to re-ignite the anti-militarism that is never far from the surface of the American psyche. The huge controversy over the alleged role of military in the fiery conclusion of David Koresh's standoff with Federal authorities at Waco, Texas, should serve as a warning in this regard. In an era when the armed forces are already struggling to recruit and retain the best and brightest, a loss of public confidence and trust would be a *real* catastrophe.

Finally, I'm convinced that terrorists can cause more harm to our way of life by forcing us to give up our civil liberties than they can by the actual damage they might do. The *San Francisco Chronicle* made this point in an editorial where it reported that "terrorist hackers" and other threats

will probably put pressure on the military to move into domestic law enforcement, blurring the line between domestic and foreign threats.<sup>53</sup>



It wisely counseled that "it is better to live with danger than in the security of a police state."<sup>54</sup> I believe that most Americans share that view, and it ought to shape the military's response as we consider the U.S.'s homeland defense policies.

## CHAPTER 12 - ENDNOTES

1. Elements of this presentation were drawn from *Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy*, Paper presented by the author at the Symposium on Cyberterrorism: "The World Held Hostage in the Digital Age," Villanova University School of Law, Villanova, PA, March 18, 2000 (copy on file with the author). A version of that presentation will be published by the Naval War College in Fall 2000.

2. Per e-mail with Michael Baxter, Insurance Institute of Indiana, March 15, 2000 (on file with author).

3. See National Highway Traffic Safety Administration, *The Economic Cost of Motor Vehicle Crashes, 1994 (1995)* Internet <http://www.nhtsa.dot.gov/people/economic/ecomvc1994.html> (accessed March 15, 2000).

4. John J. Stanton, "Rules Of Cyberwar Baffle U.S. Government Agencies," *National Defense*, February 2000, Internet <http://ebird.dtic.mil/Feb2000/s20000208rules.htm> (accessed March 15, 2000).

5. "Y2K" is shorthand for "Year 2000" and refers to the anomaly in some software programs that causes dates after 1999 to be misread, resulting in erroneous calculations. For information on the DoD program to address Y2K, see <http://www.defenselink.mil/issues/y2k.html> (accessed March 15, 2000).

6. U.S. Department of State, Office of the Coordinator for Counterterrorism, "Total International Casualties by Region 1993-1998," in *Patterns of Global Terrorism 1998 (1999)* Internet <http://www.state.gov/www/global/terrorism/1998Report/r.gif> (accessed April 11, 2000).

7. See The White House, Office of the Press Secretary, *Combating Terrorism: Presidential Decision Directive 62*, May 22, 1998 (Fact Sheet), Internet <http://www.pub.Whitehouse.Gov/uri-res/>

*12R?urn:pdi:/ /oma.eop.gov.us/1998/5/22/7.text.1* (accessed April 11, 2000).

8. U.S. Department of State, Office of the Coordinator for Counterterrorism, *U.S. Counterterrorism Policy*, Internet <http://www.state.gov/www/global/terrorism/index.html> (accessed April 11, 2000).

9. *Toth v. Quarles*, 350 U.S. 11, 17 (1955).

10. James Fallows, "Military Efficiency," *The Atlantic Monthly*, August 1991, p. 18.

11. See, generally, William S. Fields & David Hardy, "The Militia and the Constitution: A Legal History," *Military Law Review*, Vol. 1, No. 136, 1992, pp. 9-13; see also Caleb Carr, "The Troubled Genius of Oliver Cromwell," *Military History Quarterly*, Summer 1990, p. 82.

12. See, generally, Fields and Hardy, pp. 25-26.

13. See Charles J. Dunlap, Jr., "Welcome to the Junta: The Erosion of Civilian Control of the U.S. Military," *Wake Forest Law Review*, Vol. 29, No. 341, Summer 1994, pp. 342-354.

14. See, generally, Fields and Hardy, pp. 9-13; see also Carr, p. 82.

15. See, generally, Charles Fairman, *Martial Law*, Chicago: Callaghan and Company, 1943, pp. 108-116.

16. 71 U.S. 2, 1866.

17. Stephen Dycus, Arthur L. Berney, William C. Banks, and Peter Raven-Hansen, *National Security Law*, New York: Little, Brown and Company, 1990, p. 427.

18. Act of June 18, 1878, ch. 263, § 15, 20 Stat. 152 (current version at 18 U.S.C. § 1385 (Supp. 1999)).

19. Jerry Cooper, "The Posse Comitatus Act," in John Whiteclay Chambers, II, ed., *The Oxford Companion to American Military History*, 1999, pp. 555-556.

20. See, generally, David E. Engdahl, *Soldiers, Riots, and Revolution: The Law and History of Military Troops in Civil Disorders*, 57 Iowa Law Rev. 1, October 1971.

21. Loch K. Johnson, *A Season of Inquiry*, 1985, p. 223.

22. See, generally, *Ibid.*

23. See, for example, Foreign Intelligence Act of 1978, 50 U.S.C.A. §§ 1801-1811, 1991; and Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 1981 (limiting, *inter alia*, the use of intelligence agencies including those of the armed forces to collect information on persons within the United States).

24. See, for example, Department of Defense Authorization Act, Pub. L. No. 97-86, § 905(a)(1), 95 Stat. 1099, 1115 (1981), *amended by* National Defense Authorization Act, Pub. L. No. 100-456, § 1104(a), 102 Stat. 1918, 2043 (1988); National Defense Authorization Act for Fiscal Year 1990 and 1991, Pub. L. No. 101-189, § 1216(a), Nov. 29, 1989, 103 Stat. 1352, 1569 (codified at 10 U.S.C. § 371-380 (1988)).

25. The White House, *White Paper, The Clinton's Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998 (hereinafter PDD 63) press release summary available at <http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/1998/5/26/1.text.1> (accessed March 12, 2000).

26. *Ibid.*, pp. 4, 8.

27. *Ibid.*

28. The Navy has the Fleet Information Warfare Center web site available at <http://www.fiwc.navy.mil/html/home.html>, (accessed March 12, 2000), and the Army has the Information Assurance Directorate web site available at <http://www.army.mil/disc4/iseq/c2p/mission/mission.htm> (accessed March 12, 2000).

29. National Security Agency, *Mission Statement*, available at [http://www.nsa.gov/about\\_nsa/mission.html](http://www.nsa.gov/about_nsa/mission.html) (accessed April 16, 2000).

30. *Ibid.*

31. Office of the Assistant Secretary of Defense (Public Affairs), *Joint Task Force On Computer Network Defense Now Operational*, December 30, 1998, (press release) available at [http://www.defenselink.mil/news/Dec1998/b12301998\\_bt658-98.html](http://www.defenselink.mil/news/Dec1998/b12301998_bt658-98.html) (accessed March 15, 2000).

32. See Frank Wolfe, "Joint Task Force To Direct Pentagon's Cyber Defense," *Defense Daily*, January 26, 1999, p. 1, available at <http://ebird.dtic.mil/Jan1999/e19990126joint.htm> (accessed March 15, 2000).

33. U.S. Space Command, *USSPACECOM Takes Charge of DoD Computer Network Defenses*, Release No. 19-99, October 1, 1999 (press release) available at <http://www.spacecom.af.mil/usspace/new19-99.htm> (accessed March 15, 2000).

34. Douglas J. Gilbert, *High-Tech Lab Ties Computers to Crimes*, American Forces Press Service, November 1999, available at [http://www.defenselink.mil/news/Nov1999/n11021999\\_9911023.html](http://www.defenselink.mil/news/Nov1999/n11021999_9911023.html) (accessed March 15, 2000).

35. *Ibid.*

36. Linda D. Kozaryn, *DoD Helps Hometown USA Confront Terrorism*, American Forces Press Service, January 2000, available at [http://www.defenselink.mil/news/Jan2000/n01132000\\_20001133.html](http://www.defenselink.mil/news/Jan2000/n01132000_20001133.html) (accessed March 16, 2000).

37. Department of Defense, News Briefing, *Secretary of Defense William S. Cohen and Secretary of State for Defense Geoffrey Hoon*, January 27, 2000 (quoting William S. Cohen) available at [http://www.defenselink.mil/news/Jan2000/t01272000\\_t0027uk\\_.html](http://www.defenselink.mil/news/Jan2000/t01272000_t0027uk_.html) (accessed March 30, 2000).

38. 5 U.S.C.A. § 3331 (West 1996).

39. Ellis Close, "Cracks in the Thin Blue Line," *Newsweek*, April 10, 2000, p. 33 (quoting John McNamara).

40. *Ibid.*

41. See Bob Brewin, "Report: Allow Cyberwar Response," *Federal Computer Week*, March 29, 1999 (citing a report by the National Resource Council), available at [http://www.fcw.com/fcw/articles/1999/FCW\\_032999\\_255.asp](http://www.fcw.com/fcw/articles/1999/FCW_032999_255.asp) (accessed March 15, 2000).

42. *Ibid.*

43. Walter Gary Sharp, Sr., "Balancing Our Civil Liberties with Our National Security Interests in Cyberspace," *Texas Review Law and Policy*, Vol. 4, No. 69, 1999, pp. 72-73 (emphasis in the original).

44. As quoted in Patrick Pexton, "Banking on a Revolution," *Air Force Times*, September 22, 1997, p. 3.

45. Martin Libicki, "Rethinking War: The Mouse's New Roar?," *Foreign Policy*, Winter 1999/2000, p. 30. Abstract available at

<http://www.foreignpolicy.com/articles/winter1999-2000/Libicki.htm> (accessed March 14, 2000).

46. Vernon Loeb, "Cyberwar's Economic Threat," *The Washington Post*, February 24, 2000, p. 19, quoting Dan Kuehl.

47. See, for example, Brendan I Koerner, "The Web's Bad Week," *U.S. News & World Report*, February 21, 2000, p. 19. ("The intruder used an elementary method known as a denial of service attack, which cripples a network by flooding it with too much information.")

48. See Anne Plummer, "Pentagon Response To Commercial Denial-of Service Attacks Limited," *Defense Information and Electronics Report*, February 18, 2000, p. 1 (describing the denial of service attacks in early 2000 as "little more than criminal mischief").

49. See, generally, Martin Van Creveld, *Technology and War: From 2000 B.C. to the Present* (revised and expanded edition), 1991, pp. 305-306.

50. See Jim Garamone, *Hamre "Cuts" Op Center Ribbon, Thanks Cyberwarriors*, American Forces Information Services, August 1999, available at [http://www.defenselink.mil/news/Aug1999/n08241999\\_9908241.html](http://www.defenselink.mil/news/Aug1999/n08241999_9908241.html) (accessed March 11, 2000), quoting Deputy Defense Secretary Hamre ("Several times I've testified and talked about the future electronic Pearl Harbor to the United States").

51. 323 U.S. 214 (1944).

52. Sixty-eight percent of Americans said they had "a great deal" or "quite a lot" of confidence in the military. Organized religion was second at 58 percent. The Presidency and Congress were reported at 49 and 26 percent, respectively. See Tamar A. Mehuron, "Military First in Public Confidence," *Air Force Magazine*, March 2000, p. 9 (citing a late 1999 Gallup poll), available at <http://www.afa.org/magazine/chart/0300chart.html> (accessed April 5, 2000).

53. "New Terrorism Vs Individual Liberties," *San Francisco Chronicle*, September 22, 1999, p. 22, available at <http://ebird.dtic.mil/Sep1999/s19990923threats.htm> (accessed March 15, 2000).

54. *Ibid.*

## CHAPTER 13

### A STRATEGIC VIEW OF WHERE THE ARMY IS: HOMELAND DEFENSE AND ISSUES OF CIVIL-MILITARY RELATIONS

Don M. Snider,  
John A. Nagl,  
and  
Tony Pfaff

There is a proper understanding within the U.S. Army that the military must minimize its involvement in domestic affairs. Yet, the armed forces have been called on more and more to provide direct aid and support in domestic crises that range from HURRICANE ANDREW to the terrorist bombing of the Oklahoma City Federal Building. Quick, efficient, and effective responses in these and other cases have generated calls for the armed forces to take the lead in confronting the complex issues of contemporary homeland defense. The argument for this “easy fix” is straight-forward—if not quite correct. That is, the military knows how to plan for and conduct crises operations, and the federal armed forces are not hamstrung by “artificial” legal constraints, boundaries, or jurisdictions. Nevertheless, under the Rule of Law—except under the legal concept of “Necessity”—there are indeed constraints on military involvement in domestic affairs. The armed forces are not a panacea that can circumvent the American Federal Constitution.

At the same time, the Army is further constrained by some of its own problems. Because of contradictions among the missions that the Army is now expected to perform and because of the mismatch of resources provided to perform those diverse missions, the Army is in a quandary. The bottom line is that the Army is torn between “fighting the big wars” and preparing for and executing “operations other

than war." In a democracy, however, an army does not have the option of choosing the missions it accepts. The hesitancy of the U.S. Army to accept wholeheartedly the missions it is currently being given is thus cause for concern regarding its professionalism.

Professionalism, in general, is in decline within western democracies. Military professionalism is also, it appears, in decline. Professionalism is a result of at least two factors. First, it depends on the effectiveness with which the institution performs its functions. And, second, it depends on the relationship of the profession to society it serves. That is to say, the Army—among other governmental institutions—must do everything possible to do its job right and well, and to help the American public and its representatives understand that it is doing so. In this regard, it is necessary to define clearly and consistently the Army's institutional purpose and the jurisdiction of its professional work. It is also necessary to reiterate the institutional commitment to self-sacrifice on the part of its members in serving the American people and the Constitution.

Thus, this chapter will proceed to place these problems into the strategic context of military professionalism—a topic little studied in the military now and even less understood outside the profession.<sup>1</sup> We will analyze two issues within the profession now impeding healthy institutional adaptation to the new era—the officer corps' intellectual muddle over the purpose of the Army, and their ethical muddle over the role of self-sacrifice in the profession's ethos. We believe these two unresolved contradictions have contributed in very significant ways to the Army's inability thus far to deal effectively with vexing issues such as domestic defense at home and force protection abroad. We also believe that a principled approach for a renewed self-concept and motivation of the Army officer corps is an underlying theme in this analysis.

Lastly, we believe that the temptation should be resisted to give the U.S. armed forces a mandate to “lead in support” as a quick and easy solution to the contemporary problem of homeland defense. We recommend that the Army and the Department of Defense do everything possible to resolve the present “muddles” and to pursue vigilantly a long-term strategy both to perform primary war-fighting missions right and well, and to develop better relationships between our military institutions and the American society.

### Resolving the Intellectual Muddle.

After roughly 5 decades of almost continuous focus on land warfare in Europe, and now almost 1 decade of “peace,” the Army’s officer corps is, candidly speaking, in the midst of an intellectual muddle. That is, institutionally it is thinking and acting in a confused manner, one which belies its fundamental purpose and foundational relationships with the American society it serves.<sup>2</sup> Given the enormous revolutions through which American society has passed in the last decade, it should not surprise us to find that the Army is showing signs of strain; armies are such intimate reflections of their parent societies that “a revolution in the one [is] bound to cause a revolution in the other.”<sup>3</sup> Not all of the causes of this muddle are of the Army’s own making or within its control. There are, however, several important causes of the confusion that are within the institution’s control, and, as we shall explain, it is there that the Army must start to redefine its purpose and organizational essence.

*Preparing to Fight the Wrong War?* While there is much debate over whether true military innovation springs from inside organizations, from external sources, or from a combination of the two,<sup>4</sup> there is a growing recognition that cultural factors to a great extent determine whether changes accord with the organizational essence of an Army.<sup>5</sup> Clearly, during periods of significant external change, it is axiomatic that public organizations simply



cannot proceed with the learning and adaptation that is necessary for effectiveness in their task without a very clear vision of organizational essence and purpose. This is the function of senior leadership, to determine and articulate persuasively a coherent vision for the organization's future. This axiom is even more applicable to military organizations where the histories of successful innovation disclose the absolute necessity of an engaged, well-informed officer corps conceptualizing, leading, and otherwise facilitating the innovations and adaptations necessary for change. Such innovation in periods of transition is, after all, cultural in its essence rather than technological. Such clarity of vision, particularly at the strategic level, is cited by prominent theorists and historians as the essential first step of successful military innovation and adaptation—what is the new strategic task of the military institution, what is the new theory of victory for future war?<sup>6</sup> Admiral William A. Moffett had a clear vision when naval aviation was born in the 1930s, and there was no doubt in the minds of Generals Gavin and Howze after the Korean War about the new need for airmobility of Army forces. *But such clarity of vision—realistic in its premises, coherent in its components of forces, mission and resources, and thus believable to the officer corps—we believe, has not been provided since the end of the Gulf War and the initiation of the post-Cold War build-down of military capabilities.*

The two most prominent causes of the officer corps' muddle are not hard to identify. Political guidance to the Army still requires conventional capabilities to execute nearly simultaneously two major regional conflicts, hence the retention by many within the officer corps of the "big Army, big war" vision and essence, and also the retention of the bulk of the Army's Cold War force structure and infrastructure. In stark contrast, the Clinton administration has since 1993 repeatedly received the approval of the American people for the conduct of military operations other than war (MOOTW). Given the reality of a

desirable “can do” attitude among the middle and lower ranks of the officer corps, it is not surprising a significant majority of those officers now accept MOOTW missions as the purpose and essence of the Army, indeed, as the vision for the future.<sup>7</sup> They have experienced nothing else and have been presented with no other vision of the future that is credible to them.<sup>8</sup>

The major positions contributing to the muddle are shown in Figure 1.

Fighting and Winning the Nation's Wars—or Operations Other Than War?		
	Big Army, Big War	MOOTW
Political leaders	Yes	Yes
Military leaders	Yes	No . . . Perhaps <sup>9</sup> Yes (1997)
Mid-, Lower-officer corps	No, not credible	Yes

Figure 1.

As the diagram shows, America’s political leaders are telling the Army its essence is to do both big wars and MOOTW; and senior Army leaders are in turn telling the institution the same thing. But at the lower level, where the bulk of the officer corps accepts MOOTW as the way of the present and the future, it is a quite different story due to at least four other causal factors:

- The resources, both financial and human, requisite to placing both missions within the core purpose of the Army have not been forthcoming. Whether that is a failure of responsibility of political leadership or of senior military leaders is now largely irrelevant. To the majority of the serving officer corps, it is simply inconceivable, given a modernization “holiday” of almost a decade and steadily

declining funds for collective training over the same period, that senior leaders, whether uniformed or not, can expect “more with less.” In fact, this issue is one of the most frequently mentioned as cause of the unprecedented, and growing, gap in trust and confidence between the lower echelons of the Army officer corps and its senior leadership.<sup>10</sup>

- The Army’s operational tempo, caused by a 37 percent reduction in force structure since the Gulf War, coupled with repeated MOOTW, is up roughly 300 percent over Cold War levels. Army-wide, soldiers are deployed an average of over 140 days per year away from families and home post; the average is well over 200 days per year for those soldiers and families assigned within Europe. Understandably, this unsustainable rate has increasingly demoralized soldiers and their families, contributing heavily to the exodus of junior officers and, likely, to the current recruiting crisis for the volunteer force.

- The Army officer corps, until the onslaught of MOOTW in the mid-1990s, generally held the self-concept, and thus the motivation, of leader-trainers. This was the successful result of the TRADOC-led training revolution in the 1970s and 1980s.<sup>11</sup> To be an officer was to be a leader and trainer of soldiers, practically regardless of the officers’ branch. This self-concept correctly placed great emphasis on achieving positive results from rigorous training in individual and, particularly, collective skills. Unfortunately, given the multiplicity of missions and paucity of training resources currently confronting the Army, those same officers, several now in or selected for battalion and brigade command, are leaving the service in almost unprecedented numbers.<sup>12</sup> They echo the refrain, “It isn’t fun any more.”<sup>13</sup> More regrettably yet, their junior officers are also leaving, stating that “I’ve seen what my commander has had to deal with the past 2 years, and I don’t want to do that.”<sup>14</sup> *It is a sure sign of a military profession in trouble that junior officers do not aspire to serve in their commanders’ position.*

- All soldiers, regardless of rank, have watched for the past 7 years the amazing success of the American economy, but have not participated in its benefits at a commensurable rate. More importantly, sociologically this is not the Army of the 1970s or even the 1980s; roughly 60 percent of the soldiers are now married, with 85 percent of spouses working outside of the home. Thus, the impact of the excessive operation tempo on the current “married with working spouse” force has no precedent in Army history. Although some redress is on the way in FY 2000 in the form of across-the-board and focused pay increases, the failure of the Army to provide adequately for quality of life issues is cited by enlisted soldiers as the main reason—far above any other—for the lowest state of soldier morale in the 1990s.<sup>15</sup>

*These facts about the current organizational climate within the Army, particularly within the operational force structure, document the consequences of an amazingly large mismatch between resources and missions.* To be sure, there have been quantitative analyses aplenty describing the degree to which the Army lacks funding for modernization alone, and offering comparable explanations of why the Air Force is now flying the oldest fleet of aircraft in their service’s young history.<sup>16</sup> Yet until 1999, with the appearance of a systemic failure of recruiting for the volunteer force and the unremitting exodus from the Army officer corps, the magnitude of the overall danger to military professionalism was not so clear. *It is now evident, however, that the option of continuing to “muddle through” this transition is no longer an option.*

*One Solution: Fight the Wars American Society Approves.* Since this chapter is focused on problem identification and analysis rather than solutions, which are the purview of current uniformed leaders, we offer here only brief insights as to how this intellectual muddle over organizational purpose and essence might be resolved—one way among many, we are sure.

In a democracy, an Army does not get to choose the missions it accepts—at least, no professional army does. The hesitancy of the U.S. Army to accept wholeheartedly the missions it is currently being given strikes the authors of this chapter as cause for concern in the context of military professionalism. *We believe that means defining the Army's organizational purpose, its essence, simply as serving the American society, and fighting the conflicts they approve, when they approve them.* Any other essence or purpose statement places the institution in the illegitimate and unprofessional position of declaring its intellectual independence from the society it was formed to serve. And as we have deduced from the evidence presented, if the Army continues to resist organizing, training, and equipping itself to fight and win the “wars” it is currently being asked to fight, it may no longer have a sufficiently professional officer corps when the next big war occurs.

The Army can create a vision and an organizational climate that accepts the importance of MOOTW while maintaining much of its desired focus on training/adapting for future regional wars. But for that to occur, Army leaders must resolve the resources-missions gap in ways that are credible. This must be done very quickly. There are many options, from gaining relief/change in the “two-MRC” guidance, to obtaining increased resources, to reducing unneeded structure and infrastructure, to specializing roles within the total Army. None are easy nor without costs. But it is equally clear that radical action to close the gap is well past due; the cost in declining professionalism is already too great.

In light of these facts, it is encouraging that Army Chief of Staff General Erik K. Shinseki recently addressed many of the problems with which we have expressed concern in this chapter, and explicitly articulated a vision to “adjust the condition of the Army to better meet the requirements of the next century.”<sup>17</sup> That vision is clear about the need to dramatically change the Army; a vision of “Soldiers on point for the Nation *transforming* this, the most respected Army

in the world, into a *strategically responsive force* that is dominant *across the full spectrum of operations*.”<sup>18</sup>

To accomplish this transformation, General Shinseki has promised that by the end of FY 2000, the Army's divisions and armored cavalry regiments will be manned at 100 percent of authorization, removing some of the strain on units as soldiers no longer have to do the job of two or three. Even more importantly, General Shinseki established a vision of a lighter, more strategically deployable Army which will “allow us to put a combat capable brigade anywhere in the world in 96 hours once we have received ‘execute liftoff’, a division on the ground in 120 hours, and five divisions in 30 days.”

The missions to which these lighter-weight units will respond—and which their presence and capability should help to deter—are the very peacekeeping and stability operations which have confounded the Army's force structure and manning system since the end of the Cold War. General Shinseki intends to begin procuring weapons systems to man two new “middle-weight” brigades immediately. Changing the institutional culture, which still looks askance at peacekeeping missions, however, will take longer—but the need for change has been recognized, and the process has begun. It will take time to see whether this vision will prove credible and motivating to the bulk of the officer corps. As we have noted earlier in this chapter, such a credible vision has been missing, contributing to low morale and diminishing trust between officers serving in the field and their leaders in Washington. *In our view, solving the gap between missions and resources remains the unsecured, critical link to turning this new vision into more than simply another declaratory policy.*

*The Comfortable Myth of a “Casualty Averse” American Public.* Despite the promise of substantial change in the structure and organization of the Army to meet the needs of the new world order in which we find ourselves, there is a second, equally disturbing trend of incipient decline within

another component of military professionalism, the ethical component. That is the trend for senior military leaders to accept, as political leaders have accepted since the early 1990s, the myth that the American society is "casualty averse."

As we noted earlier, the issue of force protection draws some of its salience from the accepted conventional wisdom that the modern American public is very averse to accepting U.S. casualties in operations abroad. This "wisdom" is most often cited in reference to the participation of U.S. armed forces in humanitarian and peace operations. On other occasions it is presented as a broadly accepted wisdom applicable to all military operations abroad, regardless of purpose. It is a wisdom held by, and almost always voiced by, influential elites in the nation's foreign policy community, opinionmakers such as elected politicians, members of the press, columnists, and the ubiquitous chattering classes of Washington talk shows. As we shall see, not all scholars agree with this myth, particularly serious academics and serious polltakers.

The origins of such wisdom are varied, but one most often cited is the incident in Mogadishu in October of 1993. Eighteen U.S. Army Rangers were killed in that action. Live television coverage in the United States subsequently showed the body of an American soldier being dragged through the streets surrounded by jubilant Somalis.<sup>19</sup> Four days later President Clinton announced the end of U.S. involvement in the operation, ostensibly because of the public's adverse reaction to the casualties. He also announced a rapid timetable for withdrawal of all U.S. forces. The incident ultimately led to the sacking of Clinton's Secretary of Defense, Les Aspin, further heightening the understanding within the policy community that because of the public's sensitivities, casualties could not be tolerated.<sup>20</sup> At about the same time, a sociological explanation for the American public's aversion to military casualties was offered by an American scholar on the pages of one of the most prestigious journals,

*Foreign Affairs*.<sup>21</sup> Thus the myth grew—the public's intolerance of casualties results in quick reversals of public support for military operations abroad. Political leaders therefore need to factor into their foreign policy decisions the risk of such reversal, and the political costs potentially to be incurred. Subsequent political guidance to U.S. military leaders has not ceased to emphasize the urgency and importance of absolutely minimizing U.S. casualties, and by extension any collateral damage to civilian populations.

The most recent example—Kosovo, a war without a ground campaign and with U.S. pilots flying at 15,000 feet—is a clear manifestation of such political guidance. The point here is that the conventional wisdom is a myth. In fact, the American public is quite willing to accept casualties, and, doubtless, political leaders are aware of this. Recent scholarly research demonstrates, once again convincingly, that there are two conditions that must be apparent in order for the U.S. public to accept casualties:<sup>22</sup> they must be convinced there is a consensus among political leaders that the operation is in the nation's interests; and that this same consensus among political leaders is sufficient to see the venture through to a successful conclusion (Lincoln's, "that these dead here shall not have died in vain . . .").<sup>23</sup> The elite consensus was obviously missing, and thus in the public's mind so also the willingness to see it through successfully, both in the case of Somalia in 1993 and in Kosovo in 1999.<sup>24</sup> It has been the unwillingness, or inability, of the Clinton administration to create an elite consensus that leaves their policy "hostage" to the public's recoiling from the loss of American soldiers' lives. But this is not the doing of the public. Research has repeatedly demonstrated that there is room for political leaders to shape public opinion and create a forum for deliberation and debate of intervention decisions. To be sure, in that debate the public will consider in a rational calculus the risks to American lives as well as other costs and benefits of the intervention, but it is not a debate that is foreclosed because they are "casualty averse."



Therefore, if it is understood that such behavior by political leaders who as a class, and forthrightly so, are more concerned with reelection than with accomplishment of any military mission,<sup>25</sup> it becomes even more imperative to ask why senior military officers are signing operational orders with the identical guidance. As we discussed in the introduction, such is the case today with Army division commanders in Bosnia, and by implication of more senior commanders also. Is it possible that senior Army officers have adopted the policy attitudes of political leaders or, more of concern, their behavioral norms? Clearly that is the impression the junior officers have, and as well one held by those of the public interested in the issue. Even more perplexing than occasionally bowing to political pressure is senior officers' intellectual acceptance of such a myth. It is true that political leaders are going to behave as though the myth was real; it is often in their individual self-interest to do so. Thus, for practical purposes senior military leaders must accept the myth as a real influence. It is influential irrespective of its validity. But precisely because it is a myth, senior military leaders must be articulate and persuasive in advice to civilian leaders that the public is, in fact, not so casualty averse. Only then can they fulfill their profession's responsibility for candid and forthright advice to political leaders as well as their responsibility for preservation of the profession's ethic.

The gap between top military leaders and junior officers—and the public at large—is instructive here. Most mid-career officers and the American public believe that, while casualties should obviously be minimized, they remain an inevitable part of any deployment. They also believe that the accomplishment of MOOTW missions are, under certain circumstances as noted above, worth the risk of loss of American lives. This perspective is demonstrated in Figure 2.

Again, the solution appears straightforward. Senior Army leaders should replace all service guidance and doctrine that treats the prevention of U.S. casualties as

anything other than an inherent component of any operational mission.<sup>26</sup> *The trust in operational commanders' ability to accomplish missions prudently and competently, irrespective of the number of American casualties, must be restored, and immediately so.*<sup>27</sup> *Without that, few officers aware of the profession's need to maintain its own unique ethic will seek command. Ultimately there will be no profession, only an obedient military bureaucracy with no autonomy, one which responds in an unthinking and uncritical manner to the requests and directives of civilian leaders. We doubt the military effectiveness of such a bureaucracy.*

An Analysis of Casualty Aversion		
	Is the U.S. Public Casualty Averse?	Why?
Political Leaders	Yes	Intervention is High Risk
Military Leaders	Echo	High Risk; Less Preferred Form of War
Junior Military Officers	No	Willing to Sacrifice

Figure 2.

Resolving the Ethical Muddle.

Both history and present research confirm that it is during times of uncertainty and change in mission requirements that a firm foundation of shared understanding of professionalism is most needed to sustain the military organization.<sup>28</sup> We therefore offer several ideas on how to refocus individual officers, and thus the officer corps itself, on the ethical foundations of professionalism.

We turn first to the concept of self-sacrifice, specifically addressing the issue of risk as an inherent part of an officer's concept of duty. In other words, if an officer is morally obligated to lead her unit to successful mission accomplishment (the moral claim of the mission) is the obligation of, and thus the risk of, self-sacrifice inherent within that duty? And if so, what happens to the officer's moral obligation, and thus to the profession's ethic, if political leaders proscribe such risk as part of a policy of "radical force protection?" In the paragraphs that follow we address the first question by a review of the origins of the American military ethic, and subsequently answer the second by using examples of the recent NATO operation in Kosovo and Serbia.

*The Inherence of Self-sacrificial Risk: Sacrifice is not always above and beyond the call of duty.* While sacrificing may sometimes be above and beyond the call of duty, it is not always the case. We often apply words like "saint" and "hero" in a variety of situations, all of which involve sacrifice, but not all of which involve circumstances that are above and beyond the call of duty. We do call heroes people who do their duty even when considerations of self-interest or self-preservation would cause most others to fail. For example, consider the terrified doctor who remains with his patient in a plague-stricken city. Clearly he is heroic, but it is still his duty to tend to his patient. The presence or absence of the plague does not alter the fact that a doctor's duty is to remain with his patient.<sup>29</sup> It only affects how we judge the character of the doctor who does so.

Nevertheless, it is not sufficient to simply assert that there are conditions when sacrifice can be obligatory; we must spell out what those conditions are. Just as with actions in war, we must not think our concept of sacrifice must either permit everything, or allow nothing. It is hard to argue, for example, that the soldier who falls on a grenade to save his fellow soldiers was merely doing his duty. Such an action seems to be beyond the call of duty. If it is not, then it is not clear that any action ever could be. Nevertheless, it

seems equally clear that soldiers, and especially the officers who lead them, are obligated to risk their lives to accomplish legitimate missions. What remains is to give a principled account of this distinction.

In giving such an account, it is important to resist the temptation to justify such obligations by virtue of the fact that one agreed to take the job. A trucker, for example, may contract to deliver specified goods to a certain destination by a certain time.<sup>30</sup> However, he cannot be morally obligated to drive at high speeds over a dangerous shortcut, even if that means he may not be able to fulfill the provisions of the contract. The trucker, while he may have certain contractual obligations, cannot be morally obligated to put his and others' lives at risk to fulfill them. He will simply have to live with the penalty and the customer will simply have to live without the goods. The officer, however, cannot simply live without the victory that he or she may have otherwise achieved. For this reason, especially given the kinds of sacrifices that the officer is required to make, it is important that the obligation run much deeper than a mere "contract."

In fact, the obligation does run more deeply. It is rooted ultimately in the fact that the service the officer corps provides is essential if human beings are to thrive and flourish. When officers play their roles well by effectively defending a defenseless society, they are contributing to the well-being of fellow citizens. If it were otherwise, we would not be able to justify their obligation to make the sizable sacrifices officers are often called upon to make.

But these sacrifices are justified. Human beings are, among other things, social creatures. If they are to thrive, they must form the kind of societies and structures of governance that permit, if not promote, the good life for all members. In any socio-political setting, a tension arises between the needs of the community and the needs of the individual. That tension is resolved in the American constitutional system by recognizing that individuals have

certain rights, namely the right to life and the right to liberty. A socio-political setting that recognizes such rights, even if it sometimes resolves specific issues imperfectly, would be one worth defending as is the American Republic.

But rights entail obligations. If someone has a right to something, someone else has an obligation to provide for it. If a person has a right to life, the obligation falls onto someone to safeguard that life. If someone has a right to liberty, then it falls onto someone to safeguard that liberty. This is why states have an obligation to raise and maintain armies.<sup>31</sup> Armies then perform a *morally* necessary function: safeguarding the rights to which the members of that society are entitled *vis-à-vis* external threats to their security, individually and collectively.

Since it is a tragic, but no less true, fact that some human societies feel a need to destroy other human societies, it must then be a necessary feature (at least as long as this fact is true) of a good society that it be able to defend itself. This also means that it will be a good thing, though perhaps under some conditions not morally obligated, to use force to stop or prevent violent conflict, since the cessation of violent conflict is a necessary condition for a good society.

Since the authority to decide when the use of force is appropriately in the hands of the civilian authorities, professional soldiers have a *prima facie* obligation to accomplish the missions civilian authorities assign them. Since it can be morally permissible, if not obligatory, to use force outside national boundaries to stop or prevent violent conflict, professional soldiers are then obligated to perform such missions, as long as they are not blatantly immoral. As we have argued earlier, humanitarian interventions are not blatantly immoral.

Furthermore, this issue goes to the deeper issue of the ongoing redefinition in America of what it means to be a good citizen. While some may reject the idea that citizens owe any service to their country, our argument suggests otherwise. If America is a good society in the relevant sense,

then some citizens all of the time, or all citizens some of the time must either support the defense through the payment of taxes or offer themselves for service in the case of a national emergency.

And those who answer the call for service incur special moral obligations. As we have shown, what justifies these obligations is that they are necessary if the state is to be properly defended. Since a successful defense depends on successful accomplishment of certain missions, the accomplishment of those missions has moral force. This means those who undertake such missions, unlike the tardy truck driver cited earlier, are morally obligated to see them through to success—even if that means putting themselves and their soldiers at risk to do so. The only thing that could negate this is some weightier moral claim.

This obligation to sacrifice is not limited to times of conflict. Many, if not most, missions undertaken in the defense of a state engender some risk. Even in peacetime, training missions often have the potential to result in injury or death of those who participate. Thus by extension, self sacrifice on the part of the officer corps to make possible realistic training which ultimately contributes to mission accomplishment is also morally obligated.

All of this is not to say that officers can ever be indifferent to friendly casualties. Rather, it is an officer's duty to consider the risk of casualties, as well as several other factors when planning how best to accomplish assigned missions. The point is that the considerations of casualties, as well as other relevant factors, are inherent to the moral duty to defend a defenseless society.

Hence, a coherent view of the officer's duty is presented in Figure 3.

As stated before, the moral claim of the mission can only be superseded by a weightier moral claim. Self-interest, and even sometimes self-preservation, cannot serve as weightier moral claims. If they could, the possibility of



Figure 3. Coherent View of the Officer's Duty.

defending society would be undermined. And, as indicated earlier, that is not morally permissible. But, that there can be such claims must be understood before we have a complete conception of sacrifice for the military professional. The Just War Tradition (JWT), upon which the Laws of Land Warfare are founded, embody one such set of obligations. JWT recognizes that everyone has the right to life and liberty, regardless of the nation to which they belong. This right can be mitigated, even negated, but only under a certain set of conditions.

One of the fundamental principles that underlies the JWT is that soldiers are obligated to take risks to preserve the lives of noncombatants. By gaining the right to kill (which is necessary if they are to properly serve and defend the state), soldiers have given up the right not to be killed. Noncombatants have not gained the right to kill, and as such, still retain their right not to be killed. While this can be mitigated somewhat by the application of the doctrine of double effect,<sup>32</sup> that doctrine requires, among other things, that soldiers take extra risks to preserve civilian lives.<sup>33</sup>

This may seem counterintuitive to many military leaders. We often hear officers claim that their soldiers' lives are more valuable, and thus more worthy of protection, than

the lives of noncombatants.<sup>34</sup> But those who make such claims clearly misunderstand the extent of a soldier's moral obligations. A soldier exists to defend on behalf of the state the individual rights of its citizens. It makes no sense to say that soldiers, who have given up their right not to be harmed, may enjoy additional protection at the expense of the lives of civilians, who do have a right not to be harmed. Still, it is not the case that to preserve civilians' lives soldiers are obligated to take any and all risks. Their risk is limited by the following conditions: by taking this risk, (1) one cannot accomplish the mission, or (2) one will not be able to carry on future missions.

To illustrate this point, consider the following example. In World War II, French pilots flying for the Allies (over France) had the problem that if they bombed high, they could destroy their target with little risk to themselves, but at a high cost in civilian casualties. If they bombed low, they could destroy their target and their bombing would be accurate enough to minimize civilian casualties, but their casualty rate would be very high. The casualty rate would be so high, in fact, that they might be able to carry out one or two "suicide" missions, but would not long be able to sustain the effort, and the Germans would have emerged victorious. To resolve this tension, the French pilots bombed low enough to reduce civilian casualties but high enough that their casualty rates would allow for not only mission accomplishment, but also for sustained operations against the Nazis. Since all noncombatants—regardless of their nationality—retain their right to life, soldiers (or airmen in this case) are obligated to accept these extra risks as inherent within their duty.<sup>35</sup>

This illustrates well the problem a policy of radical force protection poses for the professional military ethic. Consider the recent bombing of Kosovo and Serbia, where Allied air forces bombed high enough to be out of range of Serbian anti-aircraft weapons, and Allied ground forces would not even mount a ground campaign for fear of casualties.



To our understanding, these tactics, driven by Alliance and domestic political considerations, were more designed to preserve soldiers' and aviators' lives than to rapidly and effectively accomplish the mission, thus allowing more civilian casualties than would have otherwise been the case.<sup>36</sup>

By not using Apache helicopters, A-10s, or NATO ground troops to destroy Serbian military capacity, NATO forces failed to take risks they should have taken. Certainly these forces were more vulnerable than high altitude bombers, but by keeping them out of harm's way, soldiers and aviators placed risks they could have taken onto civilians. But soldiers and aviators, as we have discussed before, are obligated to take risks, at least up to the point of certain failure, that civilians are not. If it was the case that NATO could have accepted the additional risk without dooming the mission, then NATO was obligated to do so.

By not taking the risks necessary to destroy Serb tanks and other military and paramilitary forces, NATO forces did not diminish the Serb capability to carry out their brutal policies. By aiming at Serbian infrastructure and military bases (resorting to the World War II strategy of attrition), NATO forces failed to stop the continued slaughter of innocent civilians, and, as some have argued, might have accelerated it. If this is the case, that by adopting tactics with more risk for allied soldiers they could have degraded more rapidly Serb military capacity and thereby saved innocent lives, then NATO air forces were obligated to take those extra risks. This last point is important. Under the rules of land warfare, NATO forces had at least a *prima facie* obligation to take risks to preserve innocents' lives, and they did not do so.

These tactics may have been justified if the political consequences of increased NATO military casualties would have precluded intervening on behalf of the Albanians at all. If political pressure in Germany or Italy, for example, would render NATO incapable of conducting operations

against Serbian efforts to ethnically cleanse Kosovo **AND** if failing to intervene would still result in a Kosovo cleansed of ethnic Albanians (though the cleansing would undoubtedly have proceeded at a much slower pace), then NATO's course of action, at least with respect to preserving soldiers' and airmen's' lives at the expense of rapid accomplishment of the mission, would be morally permissible. We suggest, however, that was not the case. It is quite clear that the operation could have continued as a "coalition of the willing" from within NATO, much as did the initial phases of the Bosnian campaign.

The problem for the PME should now be obvious. Servicemen and women are not only morally required to take those risks necessary to accomplish the mission, they are morally required to take some additional risks to preserve the lives of noncombatants. Even if one wants to argue that the priority mission was, in fact, force protection, the claims to the rights of life and liberty on the part of the noncombatants supersede, in this case, the moral claims of force protection as a mission. Thus, under the imposition of a policy of radical force protection we have a situation where, while serving the interests of the state, which officers are obligated to do, the state places the officer corps in a position from which it cannot fulfill its other moral obligations. This creates a contradiction that renders the professional ethic incoherent and ineffective at its most basic purpose: to provide moral guidance for behavior to both the institution and individual members.

#### A Principled Approach to Officership.<sup>37</sup>

Thus we offer the following set of principles from which all officers, and particularly those at pre-commissioning levels, should draw both their vision and their motivation.

1. The officer's duty is to serve society as a whole, to provide that which they cannot provide for themselves—security. Thus a moral obligation exists between the officer and the society he or she serves, a moral

obligation embodied in the officer's "commission." Officers act as agents of society, both individually accountable to them and, as well, serving to strengthen the claim of the service on the affections of the American people.

2. Professional officers always do their duty, subordinating their personal interests to the requirements of the professional function. They serve with unlimited liability, including life itself. When assigned a mission or task, and particularly in combat, its successful execution is first priority, above all else, with officers accepting full responsibility for their actions and orders in accomplishing it.

3. Officers, based on their military expertise, determine the standards of the profession, e.g., for tactical competence, for equipment specifications, for standards of conduct for all soldiers. Within a professional self-policing role, officers set/change the profession's standards, personally adhere to the standards, make the standards known to all soldiers, and enforce the standards.

4. The officer's motivations are noble and intrinsic, a love for his or her craft—the technical and human aspects of providing the nation's security—and the sense of moral obligation to use this craft for the benefit of society. These motivations lead to the officer's attainment and maintenance of the highest possible level of professional skill and knowledge.

5. Called to their profession and motivated by their pursuit of its expertise, officers are committed to a career of continuous study and learning.

6. Because of both the moral obligation accepted and the mortal means employed to carry out his or her duty, the officer emphasizes the importance of the group over that of the individual. Success in war requires the subordination of the will of the individual to the task of the

group—the military ethic is cooperative and cohesive in spirit, meritocratic, and fundamentally anti-individualistic and anti-careerist.

7. Officers strictly observe the principle that the military is subject to civilian authority and do not involve themselves or their subordinates in domestic politics or policy beyond the exercise of the basic rights of citizenship. Senior military officers render candid and forthright professional judgments when *representing* the profession and *advising* civilian authorities (there is no public or political *advocacy* role).

8. The officer's honor is of paramount importance, derived through history from demonstrated courage in combat—the professional soldier always fights when called on—it includes the virtues of honesty and integrity. In peace, the officer's honor is reflected in consistent acts of moral courage.

9. The officer's loyalty is legally and professionally to an office, rather than individual incumbents, and in every case is subordinate to their allegiance to the ideals codified in the Constitution.

10. The officer's loyalty also extends downward to those soldiers entrusted to their command and to their welfare, as persons as well as soldiers, and that of their families during both peace and war.

11. Officers are gentle-men and -women—persons of character, courtesy, and cultivation, possessing the qualities requisite for military leadership.

12. Officers lead by example, always maintaining the personal attributes of spiritual, physical, and mental fitness requisite to the demands of their chosen profession. Through leadership, officers invest in their subordinates, both as soldiers and as persons—and particularly in the vital non-commissioned officer corps—to the end that they grow in character, maturity and skill.

Further, we believe that the vocation of officership should be understood and executed, indeed lived, in a consistent and principled manner.

## Conclusions.

The concept of service is central to a principled understanding of officership. It holds that the profession serves the American people by providing a socially useful and necessary function: defending Americans and their interests by being schooled in war and hence able to apply effectively protective violence at their request. As noted in this chapter, this meeting of a societal need creates the moral dimension of the Army's professionalism as well as the noble character of the individual officer's service to his fellow citizens. Embodied explicitly in the commission and implicitly in the unwritten contract with society, this moral obligation requires of the officer unlimited liability, including life, as well as the moral commitment always to put service before self. Therefore, if involved in the type of crisis noted above, there should never be in the officer's mind the need to preserve self nor to take any actions at all in that direction. To the officer, self is always to be abnegated to the higher calling through the disciplined application of moral or physical courage. *A self-abnegating officer has no legacy save the character and quality of his or her service, and to attempt to create or maintain such a legacy would violate the basic concept of service inherent to the profession and to a principled understanding of officership.*

Secondly, just as the officer's commitment to service is grounded morally in his or her obligation to society, under our form of government it is also grounded in law, both in the Constitution and in subsequent statutes. But just because the commitment has two overlapping foundations does not mean that both are to be valued equally by the officer, nor equally available to the officer dealing with crisis. Particularly within an increasingly legalistic society,

the officer's reaction to crisis must always be to place fulfillment of the moral obligation over that of the legal obligation, even at personal or professional expense. His or her role must be to do the right thing, to pursue the right outcome on behalf of those served, American society. It is clear that any issue of intense divisiveness, pushed far enough by hyper-legalism and equivocation, becomes a political issue resolvable only by political means—reasoned discourse and compromise aimed, rightly, at the resolution of principled disagreements. But for the officer to pursue such resolutions is to politicize the profession, exactly the opposite of what is needed for professionalism to survive. *A principled understanding of officership requires instead that officers strive to attain the highest of moral standards, regardless of the minimum that the law might allow.*

Third, and last, is the issue of truth. Not only must commissioned officers always revere the truth, they must also never be in fear of it. The crises being discussed here do not involve truth on which there might be understandable disagreement because of epistemological concerns. The issues in political-military crises are much more mundane, but no less important—what happened, when, where, what were the causes, who responded, and how? Since the truth, as well as the absence of fear about it, cements the bond of trust between officer and society, it is always to be pursued and displayed with exceptional vigor. Utter transparency is the desired, indeed obligated, state between the accountable officer and the American people. That means as a matter of highest principal that the officer speaks “the truth, the whole truth, and nothing but the truth” at all times because he or she is perpetually under moral oath, upon accepting the commission. *Given this attitude and behavior, coupled with the concept of selfless service noted above, fear of the truth holds no power whatsoever over the officer. It is, in fact, his or her very best companion during the long journey of service.*

Thus, application of the principles yields attitudes and behavior often at odds with those within the society the

officer has chosen to serve. Does this then mean that the officer is in any manner better than those in American society? We do not believe so. It means only that the officer is different, and has unreservedly chosen to be so. Triumphalism and self-righteousness do not become the serving officer nor the profession any more than self-serving actions, appeal to legalisms, and disdain for the power of the truth. It is better, we believe, for the officers, operating in camaraderie under the imperatives of their commission, to tend in a principled manner to each other, to their profession, and to its ethos.

We trust this chapter demonstrates that we are deeply concerned by the cracks in the edifice of professionalism in the United States Army. We remain confident that a refocus on the framework of professionalism as presented here will help to correct what we see as serious corrosion, even violation, of the professional military ethic. And we are encouraged by the recent creation of a Center for the Professional Military Ethic (CPME) at the United States Military Academy, West Point. Hence we offer through that Center this chapter as a starting point for the officer corps' review, reflection, and dialogue on their, and the Army's, purpose and ethic. We believe such to be essential to help the Army refocus on its key role as the willing and effective servant of the American people.

## CHAPTER 13 - ENDNOTES

1. Portions of this chapter previously were published in Don M. Snider, John A. Nagl, and Tony Pfaff, *Army Professionalism, the Military Ethic, and Officership in the 21st Century*, Carlisle: U.S. Army War College, Strategic Studies Institute, December 1999.

2. This paper was written prior to the announcement by Army Chief of Staff General Erik K. Shinseki of his vision for reforming the Army, address to the Eisenhower Luncheon at the Association of the United States Army (AUSA) annual meeting on October 12, 1999. The arguments presented in this essay, we believe, support his vision to do just that.

3. Michael Howard, *War in European History*, Oxford: Oxford University Press, 1976, p. 75.

4. See Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*, Ithaca, NY: Cornell University Press, 1984; Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military*, Ithaca, NY: Cornell University Press, 1991; and Kimberly Martin Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955-1991*, Princeton: Princeton University Press, 1993; and Williamson Murray and Allan R. Millett, eds., *Military Effectiveness*, Three Volumes, Boston: Unwin Hyman, 1990; see also Allan R. Millett, Williamson Murray, and Kenneth H. Watman, "The Effectiveness of Military Organizations," *International Security* 11/1, Summer 1988.

5. John A. Nagl, "Learning to Eat Soup with a Knife: British and American Army Counterinsurgency Learning during the Malayan Emergency and the Vietnam War," *World Affairs* 161/4, Spring 1999; Alastair Ian Johnston, "Thinking About Strategic Culture," *International Security* 19/4, Spring 1995; Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis*, Baltimore: Johns Hopkins, 1989.

6. See Rosen; and Williamson Murray and Allen R. Millett, eds., *Military Intervention in the Inter-War Period*, London: Cambridge University Press, 1996.

7. Deborah Avant, "Officer Attitudes and Change in the post-Cold War U.S. Armed Services" in Theo Farrell and Terry Tarriff, eds., *The Sources of Military Change: Military Organisations and Their Changing Environments in the Modern Era*, forthcoming.

8. Given the paucity of resources used to exploit its unknown potential, the vision of high-technology, major-power warfare as portrayed in *Joint Vision 2010* and *Army Vision 2010* has, we believe, proved thus far to be incredible to the majority of the Army officer corps.

9. The decision in 1997 by Chief of Staff of the Army General Dennis Reimer to deploy one of the Army's premier heavy divisions, the 1st Cavalry Division, to peacekeeping duty in Bosnia can be seen as evidence that the senior leadership of the Army eventually accepted the importance of performing MOOTW missions. It can also be interpreted as evidence of the extreme stresses placed upon the institution in the post-Cold War world.



10. A multi-year study of the U.S. military will be completed in late 1999. Conducted independently by the Center for Strategic and International Studies (CSIS) in Washington, DC, but with the cooperation of the separate services, it examines empirically by field research the organizational climate within the armed forces today and recommends policies and adaptations to maintain service cultures most supportive of future military effectiveness. For a discussion of the growing "perceptions gap" between senior Army leaders in Washington and the junior grade officers in the field, see *American Military Culture in the 21st Century*, Executive Summary; and chapter 6, Center for Strategic and International Studies, forthcoming.

11. For the training revolution, see Robert K Griffith, *Today's Army Wants to Join You: The U.S. Army's Transition from the Draft to an All-volunteer Force*, Washington, DC: Center for Military History, 1995; and Anne W. Chapman, *The Army's Training Revolution, 1973-1990*, Ft Monroe, VA: Training and Doctrine Command, 1990. For recent research into the importance of self-concept in motivation and leadership, see Robert G. Lord, Douglas J. Brown, and Steven J. Friedberg, "Understanding the Dynamics of Leadership: The Role of Follower Self-Conceptions in the Leader/Follower Relationship," *Organizational Behavior and Human Decision Processes*, 78, 3, June 1999.

12. For an analysis of the impact of the reduction in officer numbers on the officer corps, see David McCormick, *The Downsized Warrior: America's Army in Transition*, New York: New York University Press, 1998.

13. CSIS, *American Military Culture*.

14. *Ibid.*

15. The data on Army morale in the 1990s is taken from, Department of the Army, *DCSPERQOL Survey*, Sept 1998-June 1999.

16. Michael O'Hanlon, "The Pentagon's Unrealistic Procurement Plans." Available at [www.brookings.edu/views/articles/ohanlon/1998af.atm](http://www.brookings.edu/views/articles/ohanlon/1998af.atm), accessed on-line.

17. All citations are from a text of the AUSA speech disseminated throughout the Army over e-mail on October 13, see footnote 1. The speech was covered by the media on the same day, drawing generally favorable reviews; see Steven Lee Myers, "Army is Restructuring With Brigades for Rapid Response," *New York Times*, October 13, 1999, p. A16.

18. Emphasis added.

19. For a thorough treatment of this incident, see Mark Bowden, *Blackhawk Down: A Story of Modern War*, New York: Atlantic Monthly Press, 1999.

20. For the relief of Secretary Aspin, see chapter 24 of Elizabeth Drew, *On the Edge: The Clinton Presidency*, New York: Simon & Schuster, 1995.

21. In fact, Edward Luttwak's theory as presented in *Foreign Affairs* was largely an assertion without empirics to support it, and has subsequently been clearly refuted. For his theory, see Edward Luttwak, "Where are the Great Powers?" *Foreign Affairs* 73, July/August 1994, pp. 23-28; "Toward Post-Heroic Warfare," *Foreign Affairs* 74, May/June 1995, pp. 109-122; and "A Post-Heroic Military Policy," *Foreign Affairs*, 75, July/August 1996, pp. 33-44. For a devastating critique of Luttwak, see James Burk, "Public Support for Peacekeeping in Lebanon and Somalia: Assessing the Casualties Hypothesis," *Political Science Quarterly*, 114, 1, 1999, pp. 53-78.

22. The recent research is: Steven Kull, "Americans on Kosovo," The Program on International Policy Attitudes, University of Maryland, May 27, 1999. This research into American public opinion on Kosovo specified a successful outcome for U.S. goals, and in turn a substantial majority of Americans responded they would continue to support the effort, notwithstanding 250 U.S. military casualties. The two conditions cited in the text have been well-known for years by public opinion scholars, most of whom also hold that the relationships between public and elite opinion are extraordinarily complex. See, for example, Benjamin I. Page and Robert Y. Shapiro, *The Rational Public*, Chicago: University of Chicago Press, 1992; and Bruce Russett, *Controlling the Sword*, Cambridge, MA: Harvard University Press, 1990.

23. See Eric V. Larson, *Casualties and Consensus*, Santa Monica, CA: Rand, 1996.

24. In contrast, Americans supported the Gulf War in 1991, fully aware of predictions of a significant number of casualties. But even then, the Bush administration barely created the elite consensus the public sought; the Senate vote to support the intervention passed only 52-48.

25. The "Mayhew hypothesis," which suggests that the first concern of any political leader is his or her reelection, was first presented in

David Mayhew, *Congress: The Electoral Connection*, New Haven: Yale University Press, 1974.

26. This issue of “radical force protection” eroding service ethics may point to a serious flaw in the Goldwater-Nichols legislation of 1986. This may be a case of political guidance and military orders flowing through joint channels of communication/command which are at serious ethical odds with the service’s Title 10 responsibilities to “man, equip and train” forces which embody an ethical culture supportive of effective warfighting.

27. It should not be lost on senior Army leaders, as it has not been lost on the Army officer corps in general, that this was one of the principled reasons for the resignation of Air Force Chief of Staff General Ronald Fogelman.

28. Andrew Gordon, “The Doctrine Debate: Having the Last Word,” in Michael Duffy, Theo Farrell and Geoffrey Sloan, eds., *Doctrine and Military Effectiveness*, Exeter, UK: The Strategic Policy Studies Group, 1997, p. 47.

29. J.O. Urmson “Saints and Heroes,” in A. I. Melden, ed., *Essays in Moral Philosophy*, 1958, pp. 199-202.

30. The authors are grateful to Colonel Anthony Hartle for assistance in developing this example.

31. See Porter, particularly chapter 7; and Huntington, particularly chapters 1 and 2.

32. Originating with Catholic theologians in the Middle Ages, the principle of double effect is the view that there is a difference between the consequences of our actions that we intend and those we do not intend, but still foresee. See Michael Walzer, *Just and Unjust Wars*, 2d ed., Basic Books, 1992, p. 152. While it has a variety of applications when applied to military situations, it explains when a military force may act in such a way as to bring about the deaths of noncombatants. The principle has four conditions: (1) the bad effect is unintended, (2) the bad effect is proportional to the desired military objective, (3) the bad effect is not a direct means to the good effect, and (4) actions are taken to minimize the foreseeable bad effects, even if it means accepting an increased risk to combatants.

33. By extra risks, we mean those risks not minimally necessary to accomplish the mission.

34. This, in fact, was Lieutenant Calley's defense during his trial for atrocities he and his platoon committed at My Lai. He claimed, "If there is one thing I am guilty of, it is valuing my soldiers' lives over that of the enemy." Since by enemy he meant more than 400 women and children, most of whom posed no threat to his unit, we can see that in fact he is claiming that no noncombatant's life was worth that of a soldier's. We can also see by this example, the absurdity of such a claim. While he may have killed, with minimal risk, some people who would later kill some of his soldiers, such an action is not morally defensible. See *Frontline* Episode, "Remember My Lai," March 5, 1989.

35. Walzer, p. 157.

36. See, "Foreign Policy: The ABC Club," *Economist*, May 22, 1999, pp. 30-31; and Michael Debbs, "Post-Mortem on NATO's Bombing Campaign," *The Washington Post National Weekly Edition*, July 19-26, 1999, p. 23. For more detail, see Paul Kahn, "War and Sacrifice in Kosovo," *Philosophy and Public Policy*, 19, 43, University of Maryland, Institute for Philosophy and Public Policy, Spring/Summer 1999, pp. 1-6.

37. This list was compiled by Dr. Snider in 1996 from multiple sources within the literature of civil-military relations, military ethics, and military professionalism. It has been improved by comments from several senior officers and refined in class discussions and research projects during 2 academic years, during which time it reached its present form.

## CHAPTER 14

### TOWARD A NATIONAL SECURITY POLICY AND STRATEGY FOR NOW AND THE 21st CENTURY

Edwin G. Corr  
and  
Max G. Manwaring

In the confusion of effort that has resulted from trying to deal with homeland defense in the complex contemporary global security environment, strategic considerations have played little part in the debate and actions pertaining to national and global security. The general result in the United States has been the ad hoc and piece-meal crisis management of security affairs. That approach, in turn, has led to ad hoc, piecemeal, and less-than-desirable results—and high personnel, monetary, and political costs. As a consequence, virtually all the contributors to this anthology either call for or respond to a call for clear policy direction—and a strategy and organizational structure that provides the basic guidance regarding how to better defend the United States and its global interests.

Separately and collectively, the contributors to this compendium analyze specific problems of national security, and implicitly and explicitly come to grips with the idea of what the Honorable John Hamre calls a unifying field theory of homeland defense. In this closing chapter, we argue that this would involve the development of a theory of deterrence to replace the theory of containment; a thoughtful reorganization of federal and state security management, coordination, and implementation structures; and farsighted research and planning mechanisms to give decisionmakers and policymakers viable political-military deterrence options as they pertain to the various discrete actors that threaten the American

homeland and American interests today. We intend to establish the philosophical underpinnings and a beginning point for a field theory from which to achieve the vision necessary for greater success in safeguarding the American homeland. In that connection, we must remember that, in the highly integrated global system, global defense is homeland defense. Finally, it is also helpful to remember that "the enemy may be us."

### The Need for a Paradigm Change.

Perhaps the greatest threat to U.S. national security is the danger that we Americans do not easily change our thinking to coincide with the changes in the world around us. America's principal defense priority for more than 40 years was the management of low-probability, high-intensity nuclear conflict, with a primary focus on Europe. Yet, ironically, nearly all the armed conflicts during that time were classified as low intensity, and took place in the Third World. Now, in addition to traditional regional security issues, an array of nontraditional threats—from proliferation of weapons of mass destruction (WMD), regional ethnic and religious conflict, a hundred different varieties of terrorism, and criminal anarchy to completely nonmilitary threats such as trade war, financial war, new terror war, and cyber war—challenge the United States at home and abroad.

The United States faces a challenge to change perspectives. We need an organizing paradigm to assist us clarifying our global leadership role, and our internal and external purposes and courses of action. One message is unmistakable. The emerging global order has given the United States the longest period of economic prosperity anyone in the current generation can remember, but the end of the Cold War era conflict did not signal the end of all global conflict. Indeed, just the reverse is proving to be true. It is becoming quite clear that if we want to preserve the present prosperity and continue to benefit from it, we must

pay for it and nurture it. Thus, U.S. interests, within the fragile and interdependent global community, demand a peace enforcer—the proverbial iron fist encased in a velvet glove. This does not mean that the United States must be directly involved all over the world all the time. It does mean, however, that the United States must rethink and renew the concept of deterrence. In much the same way that Kennan’s Containment Theory of Engagement was conceived, philosophical underpinnings must be devised for a new theory of engagement to deal more effectively with more diverse threats to the American homeland and its interests abroad from unpredictable directions, and by more diverse external and domestic state and non-state actors.

#### Some Additional Considerations that Help Define Threat and Dictate Response.

When we think about the possibilities of conflict, we tend to invent for ourselves a comfortable U.S.-centric vision—a situation with battlefields that are well understood, with an enemy who looks and acts more or less as we do, and a situation in which the fighting is done by the military—somewhere else. We must recognize, however, that in protecting our interests and confronting and influencing an adversary today, the situation has changed. We can see that change in several ways.

1. *Ambiguity.* First, the definition of “enemy” and “victory” is elusive, and the use of “power” against an enemy to achieve some form of success is diffuse. Underlying these ambiguities is the fact that contemporary conflict tends to be an intra-state affair (i.e., not an issue between sovereign states). It can be one part or several parts of one society—to include the American society—against another. Thus, there are virtually no rules. In these predominantly internal wars, there is normally no formal declaration or termination of conflict, no easily identifiable enemy military formations to attack and destroy, no specific territory to take and hold, no single credible government or political

actor with which to deal, no legal niceties such as mutually recognized national borders and Geneva Conventions to help control the situation, no guarantee that any agreement between or among contending authorities will be honored, and no commonly accepted rules of engagement to guide the leadership of a given law enforcement organization.

2. *The Need to Redefine "Enemy," "Power," and "Victory."* Second, the ambiguous political-psychological-moral nature of contemporary conflict forces the redefinition of long-used terms. The enemy is no longer a recognizable foreign military entity or an industrial capability to make war. The enemy now becomes an internal or external individual actor that plans and implements violence, and exploits the causes of violence. Power is no longer simply combat fire-power directed at a traditional enemy soldier or industrial complex. Power is multi-level and combined political, psychological, moral, informational, economic, social, military, police, and civil bureaucratic activity that can be brought to bear appropriately on the causes as well as the perpetrators of violence. And, victory is no longer the obvious and acknowledged destruction of military capability, and the resultant "unconditional" surrender. Victory, or success, is now—more and more, and perhaps with a bit of "spin control"—defined as the achievement of "peace."

3. *A "New" Center of Gravity.* These ambiguities intrude on the "comfortable" vision of war in which the assumed center of gravity has been foreign enemy military formations and his industrial capability to conduct war. Clausewitz reminds us, however, that in places subject to internal strife, the hub of all power and strength (i.e., center of gravity) is leadership and public opinion. Our energies should be directed against these. Thus, in contemporary intra-national conflict, the primary center of gravity may change from a familiar foreign military concept to an ambiguous and uncomfortable domestic leadership and public opinion paradigm.



4. *Conflict Has Become Multi-organizational, Multi-lateral, and Multi-dimensional.* Fourth, conflict is no longer a simple military to military confrontation. Conflict now involves entire populations, and parts of populations. Conflict now involves a large number of indigenous national civilian agencies, other national civilian organizations, international organizations, nongovernmental organizations, private voluntary organizations, and sub-national indigenous actors involved in dealing politically, economically, socially, morally, or militarily with complex threats to national and international security and well-being. And, those are just the “good guys.” The number and diversity of “bad guy” players can be as large. As a consequence, an almost unheard of unity of effort is required to coordinate the multi-lateral, multi-dimensional, and multi-organizational paradigm necessary for success on either or all sides of contemporary conflict. That ideal has not often been achieved in the past. Nevertheless, in the new and infinitely more complex global situation, governments, their civil and military/police components, and various other actors involved in such endeavors must find ways and means to work more effectively together.

5. *Contemporary Conflict is Not Limited; It is Total.* Finally, contemporary nontraditional war is not a kind of appendage—a lesser or limited thing—to the comfortable vision of war. It is a great deal more. As long as opposition exists that is willing to risk everything to violently take down a government, destroy a society, or cause great harm to a society—there is war. This is a zero-sum game in which there is only one winner. It is, thus, total. This is the case with domestic factions, other governments, rogue states, Maoist insurgents, Osama bin Ladin’s terrorists, the Japanese Aum Shinrikyo cult, Mafia families, Southeast Asian warlords, or Serbian ethnic cleansers—among others. This is also the case with the deliberate “financial war” attack planned and implemented by owners of international mobile capital that generated the Southeast Asia financial crisis and inflicted devastating injury on

Asia's "little tiger" countries. Their nonmilitary financial actions caused socio-economic-political devastation that could not have been exceeded by a regional war. This is also the case with the systems analyst, software engineer, scholar, or 16-year-old "hacker" that can impair the security of an army or a nation electronically as seriously as a nuclear bomb. Finally, as one more example, it must be remembered that Germany's former Chancellor Helmut Kohl breached the Berlin Wall with the powerful deutsche mark—not aircraft, artillery, armor, or infantry.

These are the internal and external deterrence realities for now and into the next century. Everything else is illusion.

Deterrence, and Preventive and Public Diplomacy.

In the anarchic environment of global politics, regardless of perceived intent, what one state or political actor does will inevitably impinge on another. That action will affect some beneficially, others adversely. Mutual dependence means that each political actor must take others into account. Interdependence affects nothing more powerfully than it does security. The result can be a vicious downward action-reaction spiral that takes the global community into instability, violence, chaos, and the inevitable destruction of stability, peace, and prosperity. As a consequence, political actors have always tried to deter others from engaging in activities considered to be harmful, or to encourage actions thought to be beneficial. A major problem in all this is that the anarchic environment of global politics allows each political actor to be the only and the final judge of his interests and actions. Again, it must be remembered that this caution also applies to illegal internal factions.

*The Primary Rules.* Here is where preventive and public diplomacy comes into play. The general rule would be that decisionmakers and policymakers must carefully calculate possible gains and losses, and when the case warrants,

apply pre-planned indirect and direct deterrent measures earlier rather than later. If done earlier, this implies the initial and intense use of low-cost diplomatic and civilian resources and military support units to ensure the deterrence message has adequate back-up. If applied earlier, preventive measures may reduce tensions that if left to fester could lead to deadly results. If done later, this normally implies the initial and intense use of high-cost military combat units to respond to a worsening situation. If applied later, preventive measures may turn out to be either irrelevant or counter-productive. Ultimately, however, the only viable test for indirect or direct preventive action sooner or later is national self-interest. In any case, the basic logic of the application of preventive and public diplomacy is unassailable—the sooner the better.

Deterrence, then, is not necessarily military—although that is important. It is not necessarily negative or directly coercive—although that, too, is important. Deterrence is not necessarily exercised against a foreign state or non-state actor—and that is very important. Deterrence is much broader than all that. Deterrence can be direct and/or indirect political-diplomatic, socio-economic, psychological-moral, and/or military-coercive. In its various forms and combinations of forms, it is an attempt to influence how and what an illegal internal or a foreign enemy or potential enemy thinks and does. That is, deterrence is the creation of a state of mind that either discourages one thing, or encourages something else. Motives and culture, thus, become crucial. It is in this context that political-psychological communication—and preventive and public diplomacy—become vital parts of the deterrence equation.

*Intermediate Rules.* In that context, the deterrence “Rule of Thumb” must move from traditional U.S.-centric values, and determine precisely what a hostile foreign or militant domestic leadership values most. The “deterrer” must then determine precisely what a hostile leadership values most—and identify exactly how that cultural

"thing"—whatever it is—can realistically be held at risk. Conversely, a new deterrence "Rule of Thumb" must also consider what a hostile leadership values most and—as opposed to the proverbial "stick"—identify precisely what "carrots" might also be offered as deterrents.

In the chaos of the "new world disorder," the threat of devastating attacks on the United States and its interests at home and abroad perpetrated by the former Soviet Union, China, and other nuclear powers still retains a certain credibility. As a result, the deterrence and preventive diplomacy task is to get into the minds of these diverse political actors, and to find viable ways and means of convincing them NOT to use nuclear or any other kind of weapons against us or anybody else in the global community. Moreover, the threats associated with the growing sophistication of biological and chemical war, and cyber war, are intensifying. At the same time, other "nontraditional" threats and menaces emanating from virtually a thousand different internal and foreign political actors with a cause—and the will to conduct asymmetrical warfare—are spreading havoc throughout the global community. And, again, the deterrence task is straight-forward. Culturally effective ways and means must be found to convince these "nontraditional" domestic and foreign players that it is NOT in their interest—whatever it may be—to continue their negative behavior.

*Advanced Rules.* Success in deterrence cannot be reduced to buying more or better military and police forces and weaponry, to superior intelligence, to genius in command, or to relative morality. Deterrence can work only if the intended deterree chooses to be deterred. There is no way that any kind of deterrence can be guaranteed. The problem is that deterrence is a dialectic between two independent wills. As a consequence, probably the single most important dimension of deterrence is clarity of communication between deterrer and deterree. As we rethink contemporary deterrence, we must not think of

ourselves as much as “warfighters” as “conflict preventers.” Thus, it is incumbent on the United States and the rest of the global community to understand and cope with the threats imposed by contemporary nontraditional actors, think “outside the box,” and replace the old “nuclear theology” with a broad deterrence strategy as it applies to the chaos provoked by the diverse state, non-state, and intra-national and trans-national nuclear and non-nuclear threats and menaces that have heretofore been ignored or wished away.

### What Is To Be Done?

The United States and the rest of the international community will inevitably face horrible new dilemmas at home and abroad that arise from the chaos engendered by the contemporary global security environment. They center on the traditional threat that stems from current and potential nuclear powers, and the many smaller—but equally deadly—nontraditional threats that are generated out of the unevenness of global integration. Clearly, the current “business as usual” crisis management approach leaves much to be desired in the context of a multi-polar world in which one or a hundred “irrational” political players are exerting differing types and levels of lethal power.

As has been suggested above, the United States needs (1) a central unifying deterrence concept to replace “containment;” (2) a thoughtful reorganization of the national and sub-national security management, coordination, and implementation structures to better deal with the complex new world; and, (3) farsighted research and planning mechanisms to give decisionmakers and policymakers viable options for deterring and/or reducing the scope, intensity, and duration of contemporary violence. Such a prioritization of effort is not a matter of “putting the strategic cart before the deterrence horse.” It is a matter of making it clear where the horse and cart are going, how they

are going to get there, and what they going to do once they arrive.

In that connection, it is important to remember that the intent of these recommendations can only be secured as a result of constant improvements in the types and levels of action we develop in pursuit of a higher quality of global and domestic stability and peace than we now enjoy. The challenge, then, is to come to terms with the fact that contemporary security—at whatever level—is at its base a holistic political-diplomatic, socio-economic, psychological-moral, and military-police effort. The corollary is to change from a singular military-police approach to a multi-dimensional, multi-organizational, and multi-cultural paradigm.

This may be accomplished within the context of a holistic implementation of direct and indirect “offensive” (i.e., proactive preventive diplomacy) and “defensive” (i.e., generally military) actions. Defensive action involves sustained coercive deterrence of threats to national interests, and, in certain instances, is relatively short-term. It primarily involves military and other civilian security efforts that are intended to stop parties in conflict from killing or moving against one another. Offensive action is generally mid to long-term. It is primarily civilian and political-economic-psychological, but is likely to have to be coordinated with defensive military or police measures. It focuses on prevention of crises, and—when appropriate—follows-up the defensive enforcement of law and order with coordinated efforts to diminish or remove the social, economic, and political causes of instability and its resultant violence. This kind of pre or post-crisis action initiates the steps necessary to reform or develop political, economic, and social institutions, procedures, and attitudes that generate the foundational elements required to address America’s central strategic vision—that of global engagement to foster legitimate civil society, economic prosperity, and durable peace.

Implementing the extraordinary challenges of reform and regeneration implied in this call for a paradigm change will not be easy. But, they are basic security strategy and national and international asset management. That will, as a result, be far less demanding and costly in political, military, and monetary terms than continuing a singular crisis management and generally military approach to global and domestic security that is inherently a long-term political problem. By accepting these challenges and tasks, the United States can help replace conflict with cooperation and to harvest the hope that a new deterrence paradigm for a more peaceful and prosperous tomorrow offers.

## ABOUT THE CONTRIBUTORS

STEPHEN A. CAMBONE is Director of Research at National Defense University's Institute for National Strategic Studies. Previously he was a Senior Fellow in Political-Military Studies at the Center for Strategic and International Studies (CSIS), and served in the Office of the Secretary of Defense as Director of Strategic Defense Policy. Previously, Dr. Cambone was the Staff Director on the Commission to Assess the Ballistic Missile Threat to the United States. He earned his B.A. at Catholic University, and his M.A. and Ph.D. in Political Science at the Claremont Graduate School. He is the author of a recent CSIS Report entitled, "A New Structure for National Security Planning; Revising the National Security Act of 1947."

GEORGE K. CAMPBELL directs Fidelity Investments' global corporate security organization. With over a trillion dollars in customer assets, Fidelity is the world's largest privately owned financial services firm. Fidelity Corporate Security performs the full range of proprietary services including information security, disaster recovery planning, background, due diligence and criminal investigations, fraud prevention, property protection, and security system engineering. Previously, Mr. Campbell owned his own security consulting firm and, before that, was a Group Vice President at a systems engineering firm supporting worldwide U.S. Government security programs. He has also served in various line and senior management functions within federal, state, and local government agencies.

EDWIN G. CORR retired from the Department of State after a distinguished career that included ambassadorships to Bolivia, El Salvador, and Peru under both Republican and Democratic administrations. He also served as Deputy Assistant Secretary of State for International Narcotics Matters, as a Peace Corps Director in Colombia, and in various posts in Thailand, Mexico, and Ecuador. Before entering the Foreign Service, Ambassador Corr served as an



infantry officer in the U.S. Marine Corps. He is currently the Director of the Energy Institute of the Americas and the Associate Director of the International Programs Center at the University of Oklahoma. Ambassador Corr is the recipient of several U.S. and foreign decorations and awards, and has written and edited various articles and books. His books include *Low-Intensity Conflict: Old Threats in a New World*.

JOHN COSTELLO is the Commanding General of the U.S. Army Space and Missile Defense Command (USASMDC), and is the Army's proponent for space and missile defense as well as the overarching integrator for theater missile defense. Additionally, Lieutenant General Costello serves as the Commanding General, U.S. Army Space Command, the Army component command to the United States Space Command. He has previously held a variety of key assignments, including service as the Director, Roles and Missions Directorate, Office of the U.S. Army Deputy Chief of Staff for Operations and Plans, and as the Assistant Division Commander for the First Armored Division. Lieutenant General Costello earned his B.A. at the Citadel, and holds a Master of Military Arts and Science degree from the U.S. Army Command and General Staff College. He has also received various U.S. and foreign decorations.

CHARLES J. DUNLAP, JR., USAF is a Staff Judge Advocate, 9th Air Force/U.S. Central Command Air Forces (USCENTAF). He most recently deployed to the Middle East to serve as the legal advisor to the Commander, USCENTAF, during Operation DESERT FOX's strikes against Iraq. Colonel Dunlap earned his B.A. in History at St. Joseph's University in Philadelphia and his Juris Doctorate from the Villanova University School of Law. He is also a graduate of the Air War College and a Distinguished Graduate of the National War College. He is widely published and speaks often on national security issues and civil-military relations.

ELLEN EMBREY is the Chief of Staff, Office of the Assistant Secretary of Defense/Reserve Affairs (OASD/RA), where she helps shape strategic and tactical efforts to influence Reserve Component structure, policies, programs, budgets, and public law to achieve national military strategy objectives. Ms. Embrey also serves as Special Assistant to the Assistant Secretary of Defense for Reserve Affairs for Military Assistance to Civil Authorities. She establishes policies, programs, plans, and budgets for National Guard and Reserve consequence management support to states, territories, and local authorities in the event of a terrorist incident involving the use of weapons of mass destruction. Ms. Embrey has more than 24 years of experience in the national security field as an analyst, administrator, and manager.

PETER D. FEAVER is an Associate Professor of Political Science at Duke University, and is currently working with the Project on the Gap Between the Military and Civilian Society that is being conducted by the Triangle Institute for Security Studies. Previously, he served as Director Defense Policy and Arms Control on the National Security Council (NSC) where his responsibilities included counter-proliferation policy, regional nuclear arms control, the national strategy review, and other defense matters. Dr. Feaver earned his Ph.D. from Harvard University and has held post-doctoral fellowships at the Olin Institute at Harvard, the Mershon Center at Ohio State University, the Council on Foreign Relations, and the John D. and Catherine T. MacArthur Foundation. He is currently finishing a book entitled, *Armed Servants: Agency Oversight and Civil Military Relations*.

JOHN J. HAMRE is the former Deputy Secretary of Defense, and is now the President of the Center for Strategic and International Studies (CSIS) in Washington, D.C. Prior to serving as Deputy Secretary of Defense, he was the Comptroller in the Department of Defense, and served for 10 years as a professional staff member of the Senate Armed Services Committee where he was primarily responsible for

oversight and evaluation of procurement, and research and development programs. Dr. Hamre earned his B.A. from Augustana College and his Ph.D. from the School of Advanced International Studies at Johns Hopkins University.

DONALD A. HAUS is Chief, Homeland Defense Division, Forces Command, Fort McPherson, Georgia. Previous assignments include tours with the executive officer to the Deputy Commander in Chief, U.S. Special Operations Command, and service as an operations officer for Special Projects with the Drug Enforcement Agency. Colonel Haus received his B.A. in Geology from the University of Tennessee at Chattanooga, holds an M.B.A. from Strayer College, and is a graduate of the U.S. Army War College.

RUSSELL HOWARD is Deputy Head of the Social Science Department at the U.S. Military Academy at West Point. Previous assignments were with the U.S. Army Special Forces in North Carolina, Somalia, and Japan. Colonel Howard holds a B.S. in Industrial Management from San Jose State University, a B.A. in Asian Studies from the University of Maryland, an M.A. in International Management from the Monterey Institute of International Studies, and a Masters of Public Administration from Harvard University.

THOMAS A. JOHNSON is Dean of the School of Public Safety and Professional Studies at the University of New Haven, in Connecticut. As a faculty member for the International Association of Police Chiefs, he teaches courses on the application of computer systems and technology in law enforcement, and on managing innovation and technology in criminal justice organizations. Dr. Johnson has served as an expert witness in state and federal courts, and as a consultant to the U.S. Department of Justice and several state law enforcement agencies. He earned his B.S. and M.S. at Michigan State University and his Ph.D. in Criminal Justice at the University of California at Berkeley. He has lectured

extensively on technology and computer applications to law enforcement, prosecution, and judicial agencies. In addition to writing two textbooks, Dr. Johnson has developed and holds the copyright to four computer software programs for various justice agencies.

MAX G. MANWARING, a retired U.S. Army colonel and Adjunct Professor of Political Science at Dickinson College, joined the Strategic Studies Institute in September 2000. He has served in various civilian and military positions at the U.S. Army War College, the United States Southern Command, and the Defense Intelligence Agency. Dr. Manwaring earned his M.A. and Ph.D. in Political Science at the University of Illinois, and is the author and co-author of several articles and reports dealing with political-military affairs. He is also the editor or co-editor of *El Salvador at War*; *Managing Contemporary Conflict: Pillars of Success*; and *Beyond Declaring Victory and Coming Home: The Challenges of Peace and Stability Operations*.

JOHN A. NAGL teaches international relations and national security studies in the Department of Social Sciences at the U.S. Military Academy at West Point. Previously, he commanded an armored cavalry troop in the First Armored Division in Germany, and led a tank platoon of the First Cavalry Division during Operation Desert Storm. A West Point graduate, Major Nagl holds Masters and Doctoral degrees in International Relations from Oxford University, where he studied as a Rhodes Scholar. His doctoral dissertation, *Learning to Eat Soup with a Knife*, examined how military organizations adapt to unfamiliar situations. Recent publications include works on arms control policy and military innovation.

WILLIAM A. NAVAS, JR., USA retired from the Army after serving 33 years as a citizen-soldier. He capped his career as Director of the Army National Guard in the National Guard Bureau of the Department of Defense. While Director, Major General Navas formulated, developed, and

coordinated all programs, policies, and plans affecting the Army National Guard. He also oversaw the Army National Guard's participation in numerous overseas deployments, and domestic crisis responses. Major General Navas received his commission in 1965 through the Army Reserve Officer Training Course at the University of Puerto Rico, and has earned numerous U.S. military awards and decorations.

TONY PFAFF teaches in the Department of English and Philosophy at the U.S. Military Academy at West Point. An infantry officer, he has served in various assignments in Macedonia for Operation Able Sentry, the First Armored Division, and the Persian Gulf with the 82nd Airborne Division. Major Pfaff received a B.A. in Economics and Philosophy from Washington and Lee University, and an M.A. in Philosophy from Stanford University. He has written and presented several papers on a variety of topics including military ethics, ethics of development, and conflict resolution.

DON M. SNIDER is professor of Political Science in the Department of Social Sciences at the U.S. Military Academy. He previously held the Olin Chair in National Security Studies at West Point, after which he became a member of the civilian faculty. A career Army officer until his retirement as a colonel, Dr. Snider's service included three combat tours in Vietnam, an assignment to the National Security Council, and a tour of duty in the Office of the Chairman of the Joint Chiefs of Staff. He is a graduate of West Point and holds a Ph.D. in Political Science from the University of Maryland.

GREGORY J.W. URWIN is an Associate Professor of History at Temple University. He won the 1998 General Wallace M. Greene, Jr., Award from the U.S. Marine Corps Heritage Foundation for his book, *Facing Fearful Odds: The Siege of Wake Island*. Dr. Urwin's other books include *Custer Victorious: The Civil War Battles of General George Armstrong Custer*, *The United States Infantry: An*

*Illustrated History, 1775-1918, and History of the 33d Iowa Infantry Volunteer Regiment, 1863-66* by A.F. Sperry (which he co-edited with his wife, Cathy Kunzinger Urwin).

U.S. ARMY WAR COLLEGE

Major General Robert R. Ivany  
Commandant

\*\*\*\*\*

STRATEGIC STUDIES INSTITUTE

Director  
Professor Douglas C. Lovelace, Jr.

Director of Research  
Dr. Earl H. Tilford, Jr.

Editor  
Dr. Max G. Manwaring

Director of Publications and Production  
Ms. Marianne P. Cowling

Publications Assistant  
Ms. Rita A. Rummel

\*\*\*\*\*

Composition  
Mrs. Christine A. Williams

Cover Artist  
Mr. James E. Kistler